SMARTLY ENGAGING SELECTED ASPECTS OF OVERALL U.S. COUNTERTERRORISM STRATEGY: AN EMPHASIS ON DOMESTIC TERRORISM, FOREIGN POLICY AND CYBERSECURITY

by
Nicholas Urbonowicz

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Government

Baltimore, Maryland
May 2021

Abstract

Not unlike the threats it strives to avert, counterterrorism strategy evolves and adapts to changing conditions. Given that terrorism is an ever-present threat to our national interests – security, prosperity, and values – one could reasonably prescribe a deductive logic-driven counterterrorism strategy whereby resources and capabilities focus on threats as they exist. In a representative democracy, elected officials or those appointed and confirmed by elected officials possess the authority to develop policies and strategies to further national interests. These men and women maintain varying worldviews, political ideologies, and specific interests that combine to influence not only how the United States contends with threats, but how it defines them. Strategies and policies are subject to varying degrees of Congressional approval and judicial review, but the simplest measurement of effectiveness may just be a measurement of elected officials' performance. Should a prevailing strategy prove ineffective, detrimental to the United States' interests, or even unpopular, its architects will face electoral consequences.

This work examines U.S. counterterrorism strategy as an aspect of domestic security, foreign policy, and cyber security, attempting to illuminate how and where politics caused otherwise avoidable setbacks that delayed or prevented the United States from achieving its basic stated objective: security. The primary contribution of this work is the development of policy prescriptions informed by reflective analysis. While this work concedes the benefit of hindsight, its conceptual guide is the idea that the past is the best light by which to see the future.

Primary Reader: Anthony Lang

Secondary Reader: Dorothea Wolfson

Contents

List of Tables

List of Figures

Introduction

> Yen Yuan asked about perfect virtue. The Master said, “To subdue one's self and return to propriety, is perfect virtue. If a man can for one day subdue himself and return to propriety, all under heaven will ascribe perfect virtue to him. Is the practice of perfect virtue from a man himself, or is it from others?” Yen Yuan said, “I beg to ask the steps of that process.” The Master replied, “Look not at what is contrary to propriety; listen not to what is contrary to propriety; speak not what is contrary to propriety; make no movement which is contrary to propriety.” Yen Yuan then said, “Though I am deficient in intelligence and vigor, I will make it my business to practice this lesson.”[1]

Over time, this Confucian anecdote has evolved into “see no evil, hear no evil, speak no evil,” but its application for the purpose of this work addresses propriety. In the hands of elected officials and those appointed by them, proper policy is a subjective concept beholden to the governing philosophies and worldviews of successive Administrations. Counterterrorism policy becomes an extension of an Administration’s grand strategy, which feeds its national security strategy.

The RAND Center for Analysis of U.S. Grand Strategy calls grand strategy a "[description of] a nation’s most important enduring interests and its theory for how it will defend or advance them, given domestic and international constraints.”[2] R.D. Hooker, Jr. distills grand strategy to eight words: “the use of power to secure the state,”[3] suggesting it exists in states’ long-term behavior; actions to achieve and advance its stated security interests. Rebecca Friedman Lissner further simplifies the concept as one of balanced “means and ends” to achieve the purposes of U.S. power.[4] Three interrelated variables influence U.S. national security policy: international political and military developments, domestic priorities, and technological advancements.[5] These variables’ dynamic nature dictates that an administration’s national security strategy is more likely to reflect Lissner’s “means and ends” definition than Hooker’s “long-term” characteristic. Thus, qualifying an Administration’s national security strategy as

grand is likely a misnomer unless the document – and the whole-of-government activities it spawns – seeks something societally significant. This paper examines the intersection of U.S. counterterrorism strategy with domestic security, foreign policy, and cyber security – how and where politics caused otherwise avoidable setbacks that delayed or prevented the United States from achieving its basic stated objective: security.

The first chapter examines domestic counterterrorism policy in the United States between 2009 and 2011 as the Obama Administration developed a community engagement model to counter radicalization and violent extremism. The United States' domestic security apparatus's inordinate focus on Arab Americans and Muslim communities provided rightwing extremist groups the requisite space and time to operate. Even with the benefit of hindsight, it is difficult to assess whether this avoidable outcome was the result of treating domestic national security as a mirror-image of global U.S. counterterrorism efforts or willful ignorance of the veracity of rightwing extremist groups as a threat. Nonetheless, the U.S. Intelligence Community's March 2021 assessment that domestic violent extremists motivated by racist and antigovernment biases "pose an elevated threat" to homeland security in 2021 merits an examination of 2009 to 2011,[6] if for nothing more than to identify the point at which the United States lost focus on a credible threat. This chapter seeks not to assign blame, merely to highlight the societal and security consequences of the United States' swerve in an attempt to avoid a repetition of history.

The second chapter examines counterterrorism as a component of U.S. foreign policy in East Africa, focusing on the Obama and Trump Administrations' efforts against al-Shabaab in Somalia. By examining the degrees to which each Administration applied hard and soft power and incorporated counterterrorism into its respective strategies for East Africa and Africa writ-large, this chapter seeks to identify the correct balance of what Joseph S. Nye refers to as *smart*

power. While the chapter addresses the performance and effectiveness of the Administrations' counterterrorism operations, its focus is the extent to which each Administration leveraged counterterrorism as a means by which to further broader strategic objectives such as regional stability, countering violent extremism and radicalization, development, and great power competition for influence. With the latter objective's preeminence in contemporary U.S. national security and defense strategies,[7] policymakers may be inclined to deemphasize the role of counterterrorism operations. This is understandable from a resource management perspective in the face of budget constraints and competing priorities. However, counterterrorism or security operations conducted in proximity to strategic competitors are opportunities to leverage access and placement from which to illuminate malign activity through information operations. As part of an overarching strategy of great power competition, a smart power approach in which counterterrorism plays a limited role could provide a foothold for strategic competition and concurrently improve regional stability – all while enhancing perceptions of the United States.

The last chapter examines the lack of coherence over U.S. cybersecurity policy, concluding that a lack of centralized Executive authority and Congressional oversight create a strategic vulnerability that must be addressed as part of a comprehensive counterterrorism policy. Similar to the previous chapter's prescription that counterterrorism is simply an element of foreign policy and should not serve as the driving force behind U.S. policymakers' decisions, this chapter encourages a point of view whereby the U.S. government addresses cybersecurity with the same tenacity that it treats counterterrorism. The indispensability of critical infrastructure and its related services to Americans citizens' daily lives merits a coherent approach to its protection and resiliency on par with national security systems. An examination of Executive organizational models for cybersecurity from the United Kingdom and Australia

provide helpful examples for the United States, but this chapter ultimately concludes that a centralized authority over government cybersecurity is effectively limited without a complementary legislative mandate.

Rather than focusing on the newly created National Cyber Director in this regard, the chapter asserts that the more pressing need lies in strengthening the Cybersecurity and Infrastructure Security Agency, particularly with respect to its authority over private sector critical infrastructure. The idea of a regulatory agency empowered to institute mandatory cybersecurity standards on private companies is no doubt antithetical to laissez-faire capitalism. As a rule, it should be perfectly acceptable for a private American business owner to favor *Atlas Shrugged* over the reality of cyber threats, but the indispensable nature of critical infrastructure presents an exception.

This work began in 2014 as a laudatory examination of fusion centers as an aspect of Obama Administration domestic counterterrorism strategy to counter violent extremism, but a combination of personal and professional factors caused a change in view and direction for the overall piece. First came a question about the utility of simply applying an overarching counterterrorism strategy both internationally and domestically, as the latter appeared to only focus on defensive measures against threats identified in the former. Radicalization was and remains a potent threat, but assigning it exclusivity seemed myopic. Second, a more holistic view of U.S. efforts to counter violent extremism produced more familiarity with their detrimental effect on minority communities. Finally, questions about the efficacy of counterterrorism strategy in a domestic context engendered a curiosity to seek similar shortcomings in other areas of national security. Each chapter shows a progression of counterterrorism strategy in each area, identifying areas for improvement in future strategy.

Notes

1. Confucius, "Book XII, YEN YUAN," in *The Analects of Confucius (from the Chinese Classics)*, trans. James Legge (Project Gutenberg, n.d.), Chap. I. 1, https://www.gutenberg.org/cache/epub/3330/pg3330.html.

2. "Center for Analysis of U.S. Grand Strategy," RAND, October 25, 2020, https://www.rand.org/nsrd/isdp/grand-strategy.html.

3. R.D. Hooker, *The Grand Strategy of the United States* (Washington, DC: National Defense University, 2014), 1, https://apps.dtic.mil/dtic/tr/fulltext/u2/a610607.pdf.

4. Rebecca Freidman Lissner, "The National Security Strategy Is Not a Strategy," *Foreign Affairs*, December 19, 2017, https://www.foreignaffairs.com/articles/united-states/2017-12-19/national-security-strategy-not-strategy.

5. Michael J. Meese, Suzanne C. Nielsen, and David Kasten, *American National Security*, 7th ed. (Baltimore: Johns Hopkins University Press, 2018), 52-54.

6. Office of the Director of National Intelligence, *Domestic Violent Extremism Poses Heightened Threat in 2021* (Washington, DC: Office of the Director of National Intelligence, 2021), 2, https://www.odni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf.

7. "DoD China Task Force Announcement," Department of Defense, 2021, https://www.airforcemag.com/app/uploads/2021/02/DoD-Fact-Sheet-China-Task-Force-10-FEB-2021.pdf.

Chapter 1: Ignoring the Threat

Released nearly ten years after the September 11, 2001 terrorist attacks, the Obama Administration's *National Strategy for Counterterrorism* identifies "al-Qaeda and its affiliates and adherents" as the United States' "preeminent security threat."[1] Like all states' national security strategies, the *National Strategy for Counterterrorism* strives to protect the United States, its citizens, and its interests. Because al-Qaeda is a global entity, the offensive aspects of the United States' strategy to "disrupt, degrade, dismantle, and defeat"[2] its preeminent threat occur primarily outside of the United States through military and intelligence operations. Reflecting an external threat, the strategy's domestic component outlines a defensive posture whereby enhancements to aviation and border security "harden" the United States to deny terrorists access and freedom of movement.[3] Existent terrorist threats within the United States are only presented in the context of al-Qaeda; affiliates or adherents either plotting attacks or inspiring others through radicalization. Addressing the latter became the cornerstone of the U.S. government's domestic strategy for counterterrorism; proactive engagement of communities to counter violent extremism (CVE) by reducing polarization and mistrust.

If fusion centers' effects were the result of local expertise, it stands to reason that a granular approach to CVE would reduce threats to an extent comparable to overseas military and intelligence operations, albeit in a domestic context. However, as an aspect of a whole-of-government counterterrorism strategy identifying al-Qaeda as its primary focus, the United States focused primarily on its Arab-American community. In its attempt to *proactively* counter terrorist threats by attacking radicalization, the United States effectively extended its *reactive* posture after the attack by al-Qaeda on September 11, 2001. At the policy-level, this singular focus on al-Qaeda betrayed a blind spot for a wholly organic threat: rightwing extremism.

*

The Obama Administration's CVE strategy, the *National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States* ("*Empowering Local Partners*") illustrates this point by presenting "neo-Nazis and other anti-Semitic hate groups, [and] racial supremacists" as a historical footnote before the emergence of al-Qaeda.[4] Nonetheless, from September 12, 2001 to the August 2011 release of *Empowering Local Partners*, far right extremists committed more than twice as many violent attacks in the United States as radical Islamists: 49 incidents resulting in 63 deaths, compared to 21 incidents resulting in 38 deaths, respectively.[5]

This chapter examines the inception of U.S. CVE strategy, contending that its implementation as the domestic pillar of a broader counterterrorism strategy focused on external threats created a cognitive bias by which the Arab American community became the only logical venue in which to counter violent extremism in the United States. This swerve afforded time and space to far right extremist groups whose cultural identities and citations of Constitutional rights to speech and firearms proved more sympathetic to the body politic. In the face of demonstrable evidence of this threat, the U.S. government seemed to view it as an unworthy source of violent extremism to counter. Ten years after the release of *Empowering Local Partners*, the January 6, 2021 attack on the U.S. Capitol by insurrectionists is a catalyst to consider the missed opportunities of U.S. CVE strategy. That scores of violent incidents by far-right extremists occurred while the U.S. government labored to counter violent extremism suggests a similarity to

* A Department of Homeland Security reference aid titled *Domestic Extremism Lexicon* defines *rightwing extremism* as "a movement of rightwing groups or individuals who can be broadly divided into those who are primarily hate-oriented, and those who are mainly antigovernment and reject federal authority in favor of state or local authority." The term also applies to "rightwing" extremist movements that are dedicated to a single issue, such as opposition to abortion or immigration."

the disconnected U.S. counterterrorism strategy prior to September 11, 2001: "the system was blinking red."[6]

The Threat as a Constituency

In February 2009, the Missouri Information Analysis Center (MIAC) – a fusion center – released a report titled *The Modern Militia Movement*, noting a reemergence of rightwing extremist militias spurred by conspiracy theories, high unemployment rates, and the election of the first African American President of the United States, likening these environmental factors to those present during the surge in U.S. militia activity in the 1990s.[7] By drawing interdecadal parallels between groups' tactics and targets, the MIAC report asserts that such groups never actually dissolved; their reemergence could more accurately be described as society's renewed attention. In April 2009, DHS released a similar assessment from its Office of Intelligence and Analysis – the Department's component of the Intelligence Community (IC) – by the Extremism and Radicalization Branch of the Homeland Environment Threat Analysis Division. Adhering to IC policy for disseminating threat information concerning homeland security,[8] the report's distribution included "federal, state, local, and tribal counterterrorism and law enforcement officials so they may effectively deter, prevent, preempt, or respond to terrorist attacks against the United States."[9] *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment* ("*Rightwing Extremism*") credits economic and national political factors with fueling an increase in recruitment by- and radicalization toward rightwing extremism.[10] Both reports sought to highlight ideological, behavioral, and organizational trends of rightwing extremist groups for law enforcement agencies. Their publication sparked a national outrage causing their agencies to deprioritize rightwing extremism. Conservative politicians and media outlets fueled a political narrative by fixating on

specific aspects of each report, eventually delegitimizing both without disputing or even addressing the theses.

The Modern Militia Movement was not produced by the IC, yet the latter's reporting standards are nonetheless a helpful resource by which to assess the quality of an intelligence assessment. Whereas the IC directs that disseminated analytical products "shall contain sourcing information…to optimize clarity and reader understanding,"[11] the MIAC report contains no sourcing. The report fails to distinguish between information-based assertions and analytical assumptions, offers no description of the methodology used to reach its conclusions, and contains spelling errors; all contrary to basic analytic standards.[12] While these issues were problematic, MIAC's critics generally overlooked the quality of the report, focusing instead on its conclusions about militia members' political preferences. According to MIAC, "militia members most commonly associate with 3rd party political groups" such as the Constitutional or Libertarian parties, and support politicians such as "Ron Paul, Chuck Baldwin, and Bob Barr."[13] If a militia member who fears and expansive government and espouses personal liberty is inclined to vote in a national election, it stands to reason that he or she will vote for a candidate who articulates those positions. The connection seems obvious, but the report fails to articulate its relevance to law enforcement, seemingly implying that political affiliation is an indicator of extremist tendences. A 2012 report by the U.S. Senate Permanent Subcommittee on Investigations (PSI) describes the MIAC report's fundamental weakness as "[attempting] to show connections between certain Constitutionally protected, non-violent political activity and a tendency towards violent extremism."[14] Insofar as a criticism of the MIAC report's style and substance, PSI's comments are valid; the report was an imperfect messenger.

Rightwing Extremism met a similar fate, primarily stemming from its conclusion that "rightwing extremists will attempt to recruit and radicalize returning veterans" to enhance their groups' capabilities.[15] Its lack of sourcing left it vulnerable to the same flavor of attacks as the MIAC report, albeit on a national level. David K. Rehbein, the national commander of the American Legion, published an open letter to Homeland Security Secretary Janet Napolitano taking issue with the report's use of the "stereotypical 'disgruntled military veteran,'" pointing to a lack of statistical evidence to support its conclusions.[16] Conservative politicians and activists echoed Rehbein's sentiments, with then-House Minority Leader Representative John Boehner insisting that DHS "owes veterans an apology."[17] While Napolitano ultimately capitulated and issued an apology, her department's subsequent actions spoke louder than the Secretary's words.

Two months after DHS's repudiation of *Rightwing Extremism*, the author of an anti-Semitic website embarked on a shooting spree at the U.S. Holocaust Museum in Washington, D.C.,[18] followed by the assassination of an abortion doctor in Kansas.[19] Despite these and a series of similar attacks across the United States, DHS began internally deprioritizing domestic extremism by cutting analytical staff.[20] By 2011, the department had effectively ceased releasing in-depth reports about domestic extremist groups and routinely prevented personnel from briefing state and local officials about domestic extremist groups.[21]

Countering Violent Extremism

Between 2009 and 2010, seventy U.S. citizens were either charged with- or convicted of terrorism or related crimes. In an assessment of European CVE initiatives to seek lessons-learned for the United States, Lorenzo Vidino suggests that this surge likely caused the United States to "question the long-held assumption that American Muslims are immune to radicalization," thus requiring a comprehensive counter-radicalization strategy similar to those of "other Western

democracies."[22] Vidino attributes European nations' successful counter-radicalization efforts to "strong trust-based partnerships with individuals and organizations" within their respective Muslim communities.[23] In February 2010, Napolitano tasked the Homeland Security Advisory Council to develop recommendations for how DHS could combat violent extremism at the community level. Applying violent crime prevention techniques, the Council concluded that stopping ideologically motivated crime at the community level requires relationship- and information-driven engagement.[24] These recommendations would become the basis for *Empowering Local Partners*. The strategy was three-pronged:

1. Enhance federal engagement with and support to local communities that may be targeted by violent extremists.
2. Build government and law enforcement expertise for preventing violent extremism.
3. Counter violent extremist propaganda while promoting the United States' ideals.[25]

Empowering Local Partners identifies community-level efforts as "best placed to recognize and confront the threat because violent extremists are targeting their children, families, and neighbors."[26] This is a reasonable approach to countering threats, but focusing on a single community creates the obvious risk of missing threats emanating from other communities, thereby precluding law enforcement and intelligence agencies from learning about emerging threats. Furthermore, nothing about far-right extremists in the United States during this period should have been considered emergent.

Federal Engagement with and Support to Vulnerable Communities

By ostensibly distinguishing its efforts from a broader counterterrorism strategy, the U.S. government attempted to avoid focusing community-level dialogue to CVE. *Empowering Local Partners* notes that the "vast majority of [its] engagement work relates to issues outside the national security arena, such as jobs, education, health, and civil rights," [27] by leveraging many of the same tools already being employed to counter the appeal of gang recruitment by youth

service organizations. Engagement sought to remove any lingering reservations of those on whom CVE efforts must rely, thereby allowing for the establishment of mutual trust. While implementation was a whole-of-government effort, the Departments of Justice and Homeland Security, and the Federal Bureau of Investigation (FBI) executed most of the strategy's initiatives. This separation had the potential to remove the suspicions of community leaders that could otherwise prevent the underlying objective for "government and communities to share information, concerns, and potential solutions."[28]

A successful instance of this is the April 2015 arrest of six Somali Americans in San Diego and Minneapolis on charges that they were conspiring to travel to Syria in order to join the self-proclaimed Islamic State (ISIS). A family contacted Abdirizak Bihi, director of Somali education at the Social Advocacy Center in Minneapolis "because their son was acting weird…and he wanted to get a passport."[29] Bihi immediately placed the family in contact with the local police department, which relayed the information to federal authorities with the reach to effect the arrests in San Diego and Minneapolis. Along with Minneapolis, Boston and Los Angeles hosted programs aimed at curbing community-level Islamist radicalization.

Building Government and Law Enforcement Expertise for Preventing Violent Extremism

Bearing in mind the accepted wisdom that radicalization is begins at the community level, each instance of an individual radicalizing should present a series of circumstances specific to either that individual or the community. The United States has established, DHS, regional fusion centers in major urban areas to serve as "analytic hubs" through which to "empower frontline personnel to understand the local implications of national intelligence by tailoring national threat information into a local context."[30] In this sense, fusion centers provide an avenue through which the federal government can filter intelligence to local elements that are better-

suited to interpret threat information as it applies to specific communities. On the other hand, fusion centers represent the United States' means of "educating and informing state and local partners on behaviors and indicators of potential threats."[31] By providing both (community-specific) intelligence *and* training to identify radicalization vulnerabilities and/or indicators of potential terrorist activity, fusion centers create a link between the United States' national intelligence apparatus and local law enforcement; a top-to-bottom approach to counter-radicalization.

An operational success story involving the North Carolina Information Sharing and Analysis Center (ISAAC) demonstrates the intersection of fusion centers and community engagement. In August 2009, information developed through ISAAC's community outreach program – an effort to increase public awareness of the center and its mission – uncovered a group of extremists in a rural area south of Raleigh, North Carolina.[32] Daniel Patrick Boyd was arrested for attempting to recruit individuals to advance violent jihad; he and seven members of his group were ultimately convicted of funding, training, and recruiting militants overseas.[33]

In September 2009, the Colorado Information Analysis Center (CIAC) supported an investigation of a missing Colorado woman whose mother indicated that her daughter had converted to Islam after communicating with a Pakistani man over the Internet, and was travelling to New York to meet the man. After receiving the information in Colorado, the CIAC notified the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF), which subsequently opened an investigation of Jamie Paulin-Ramirez. In March 2010, Paulin-Ramirez and five others were detained in Ireland in connection with a terrorist conspiracy to kill a Swedish cartoonist who had portrayed the prophet Muhammed as a dog in a cartoon. Simultaneously, in an unrelated investigation of Colleen R. LaRose (a.k.a. "Jihad Jane"), the FBI

discovered an Internet communication between Paulin-Ramirez and the suspected terrorist Najibullah Zazi, who pleaded guilty in February 2010 of planning to bomb the New York City subway system.[34] To be certain, Fusion Centers represent a more efficient use of law enforcement resources against potential terrorist threats; clearing houses of information which transcend typical jurisdictional boundaries. This fact alone would make fusion centers potent forces to counter right-wing extremist groups, which makes the latter's diminished priority even more confounding. The concept of federalism notwithstanding, prioritizing Arab-American communities represented a national security priority.

In February 2015, the Obama Administration held a summit on Countering Violent Extremism (CVE) to mark the beginning of the United States' efforts to counter polarization and mistrust within communities.

> Yesterday at the White House, we welcomed community groups from the United States, and from some of your countries, to focus on how we can empower communities to protect their families and friends and neighbors from violent ideologies and recruitment. We must acknowledge that groups like al Qaeda and ISIL are deliberately targeting their propaganda to Muslim communities, particularly Muslim youth. And Muslim communities, including scholars and clerics, therefore have a responsibility to push back, not just on twisted interpretations of Islam, but also on the lie that we are somehow engaged in a clash of civilizations; that America and the West are somehow at war with Islam or seek to suppress Muslims; or that we are the cause of every ill in the Middle East. That narrative sometimes extends far beyond terrorist organizations. That narrative becomes the foundation upon which terrorists build their ideology and by which they try to justify their violence. And that hurts all of us, including Islam, especially Muslims, who are the ones most likely to be killed.[35]

The summit was three-pronged: focusing on multi-faith efforts within the United States to counter polarization, a global discussion including representatives from European and African nations familiar with these issues, and efforts by the United States to counter the radicalization and recruitment of U.S. residents. By this point – almost six years after Secretary Napolitano apologized for *Rightwing Extremism* – the United States' mechanisms for community-level

engagement to counter domestic extremism had completely swerved away from rightwing groups in favor of something better-aligned with its broader counterterrorism objectives.

Arab-Americans

Prejudice, discrimination, and violence against Arab-Americans (and Muslims) dramatically increased drastically after the September 11, 2001 attack(s) on the United States. September 11 created a shift in how the American psyche views the Middle East and how it treats individuals within the United States who have Middle Eastern heritage and affiliation; an entire ethnic group was immediately placed at risk and in danger of discrimination and prejudice. In the years following September 11, U.S. military and paramilitary activities throughout the Arab World have deepened the chasm of suspicion of Arab-Americans in the United States. The scope and breadth of this chasm is manifest in hate crimes, both silent and vocal concerns of travelers in mass transit, and political rhetoric. Whatever the manifestation(s), the root and stated cause is a desire for increased national security during the United States' targeting of "terrorism." While achievements by the United States in foreign and domestic theaters have returned results in the form of strengthened national security, the lasting effect has been to the detriment of Arab-Americans; a prolonged suspicion and the concept of "us versus them."

Arab Americans constitute an ethnicity made up of several waves of immigrants from the Arabic-speaking countries of southwestern Asia and North Africa that have settled in the United States since the 1880's; eighty percent of whom are American citizens. The cultural roots of this ethnic group span twenty-two countries: Mauritania, Morocco, Algeria, Tunisia, Libya, Egypt, Sudan, Lebanon, Palestine, Jordan, Syria, Iraq, Kuwait, Saudi Arabia, Bahrain, Qatar, United Arab Emirates, Oman, Yemen, Djibouti, and Somalia.[36] The immigration of Arab Americans to the United States primarily occurred in two waves. The first wave took place from 1890-1940,

consisting primarily of economically motivated Christian merchants and farmers seeking jobs. Similar to the millions who left their homes in Europe during late nineteenth century, these immigrants embarked traveled to North America in search of prosperity – overwhelmingly consisting of unsophisticated village farmers and/or artisans who were relatively poor and uneducated.[37] The large tracts of uncultivated land in the American West and Southwest served as ample motivation for agrarian-minded immigrants. The second, post-World War II wave differed greatly from the first in that it contained a large component of educated and bilingual immigrants. The politicized and nationalistic ideals carried by this wave of Arab immigrants sprung from their having originated from numerous Arab nations that gained their independence following World War II.[38] Distinguishing the first wave from the second is critical to understanding the origins of Arab American identity; the second wave carried with them a sense of national (and ethnic) pride that translated into self-identification as "Arab."

In its annual report of hate crime statistics, the FBI reported a 1600 percent increase in "anti-Islamic" incidents in 2001; from 28 incidents with 36 victims in 2000 to 481 incidents with 554 victims in 2001[39†]. Similarly, in a population-based survey of Middle-Eastern Arabic-speaking adults in the United States, approximately thirty percent of Arabs and fifty percent of Muslims reported discrimination in the eight months after September 11.[40] Two years after the September 11 attacks, fifteen percent of Arab Americans in the Detroit area reported harassment or intimidation due to their ethnicity; verbal insults, workplace discrimination, targeting by law enforcement or airport security, vandalism, and vehicular and/or physical assault.[41] Twenty four percent of those polled reported that they or a member of their household suffered a verbal insult

† While the "anti-Islamic" incidents are significant, also of note is the quadruple increase in "anti-other ethnicity/national origin" category, as this denotes incidents against Arab Americans, not necessarily motivated by anti-Islamic sentiment(s).

due to their ethnicity or religion, while thirteen percent reported threatening gestures.[42] An astonishing forty-two percent of Arab Americans interviewed for the survey in Detroit, an area with one of the highest concentrations of Arab Americans in the United States, felt their religion is not respected by mainstream society. It is important to differentiate the post-September 11 figures regarding attitudes and perceived insecurity on the part of Arab Americans in the face of hate crimes and/or discrimination as responsive to individual incidents versus an institutional framework of ethnic prejudice.[43]

The most flagrant example of institutional prejudice against Arab Americans lies within the New York City Police Department's (NYPD) post- September 11 secret intelligence operations. The NYPD would subject entire neighborhoods to surveillance and scrutiny based upon the ethnicity of the residents. Hundreds of mosques and Muslim student groups were investigated and/or infiltrated by undercover NYPD officers and informants in a practice known as "mosque crawling."

Figure 1. Egyptian Locations of Interest Brooklyn

In a July 7, 2006 NYPD document obtained by the Associated Press (Figure 1), the NYPD's Demographics Unit identified business districts and population centers within the various Egyptian communities of New York City in order to "gauge the general sentiment of the community" and gain "insight into the general activity" of the community.[44] The NYPD defined these "locations of interest" as:

- Localized center(s) of activity for a particular ethnic group.
- Location that persons of concern may be attracted to.
- Location that individuals may frequent to search for ethnic companionship.
- Location that individuals may find co-conspirators for illegal actions.
- Location that has demonstrated a significant pattern of illegal activities.
- Location that can be used as a listening post.
- Popular hangout or meeting location for a particular ethnic group that provides a forum for listening to neighborhood gossip or otherwise provide an overall feel for the community.

If one considers the NYPD's Demographic Unit solely as a surveillance component within a larger counterterrorism strategy, it is likely a success. The program thwarted a plot to bomb the New York City subway system in 2004 and discovered two men on their way to receive terrorism training in Somalia.[45] Thus, its efficacy makes a compelling case for the continuation of similar programs. However, the effect the unit's operations will have on the psyche of Arab Americans in New York City is likely similar to those of Seattle residents in response bus advertisements detailing the "faces of terrorism" for the Department of State's Rewards for Justice Program.[46] Using language similar to that of her colleague Congressman McDermott, Congresswoman Yvette Clark of New York City noted that the NYPD's efforts should not include "singling out specific ethnic or religious groups."[47] A fundamental weakness of the NYPD Demographics Unit was the absence of a transparent CVE program running concurrently.

"Victories" by the Rewards for Justice Program or the NYPD Demographics Unit have likely come at the expense of the emotional well-being of Arab Americans by perpetuating the idea that Arabs or Muslims – as ethnic and religious groups, respectively - are a threat to national security. This makes the government an unwitting accomplice to both the perpetuation of related stereotypes among the American people and in part, persistent hate-crimes against Arab Americans. Racial and ethnic discrimination is associated with increased psychological distress and anxiety, increased risk for adverse mental health outcomes, and poorer health status.[48] Furthermore, immigrants who perceive increased discrimination in their new country are more likely to have high levels of psychological distress and decreased levels of trust in society.[49]

In a 2003 study exploring the impact of September 11 on the Arab American community, Wahiba Abu-Ras and Soleman H. Abu-Bader, employing a focus group methodology, interviewed 83 total participants in Brooklyn, NY. According to the participants in the study, most Arab Americans have experienced three related traumas: the September 11 terrorist attacks, increased hate crimes, and targeting by new immigration laws and policies – all of which have generated a sense of "loss of community."[50] Accompanying the loss of community, an overwhelming sense of fear and anxiety were reported; one participant attributed this anxiety to the way that Americans perceive Arabs: "They look at us as enemies and not as American citizens. We become the ones blamed for any terrorist activities inside and outside the U.S."[51] Perhaps most tellingly, the single biggest concern identified by participants was "safety," quantified by an imam as "not only to be physically and mentally protected, but to have family stability, to be safe and protected from all institutionalized laws and policies that have been aggressively created and practiced against the Arab community."[52]

Al-Qaeda's Ayman al-Zawahiri once declared that "more than half of this battle is taking place in the battlefield of the media," seemingly testifying to the rapid technological advancements and subsequent notoriety brought-about by social networking and audience-specific content. John M. Venhaus notes that the "central tenet" of a counter-radicalization strategy is "to discredit the brand image and dissuade those who seek membership and affiliation" with violent Islamist organizations.[53] Venhaus suggests that by accompanying the physical confrontation of counterterrorism operations (by military, intelligence, and law enforcement entities) with a "parallel effort" of discrediting the messaging of groups like al-Qaeda could lead to a "psychological defeat".[54] While this is a component of information operations directed overseas by entities like the Global Engagement Center, it deserves an inward-facing domestic component – not propaganda – achievable by community engagement.

Reprioritizing Local Efforts

A state's policy of "how" and "where" to counter radicalization – its allocation of engagement resources to specific communities, training local law enforcement elements, or countering extremist propaganda – must be driven by a sober, apolitical assessment of the threat environment. No aspect of CVE efforts is achievable without community-level engagement with civic leaders, religious leaders, and youth service organizations – everything in the realm of federal activity within communities must be implemented through these avenues. Close relationships at the community-level have the potential to diminish suspicions on the part of the needed community leaders. The strengths of the United States' CVE approach will ultimately lie in its ability to successfully balance the small with the large; the gargantuan amount of federal government assets (intelligence, defense, fiscal) must be strategically applied to communities through well-managed outreach efforts. The strategic application of these efforts will directly

affect the CVE programs, as their efficacy will inevitably be tied to their ability to manage and overcome the reservations of those to whom the very programs are designed to address. This will require a dynamic of cultural awareness on the part of law enforcement entities that is best aided by the input of community leaders and complemented by appropriate training.

To be sure, the nineteen hijackers who perpetrated the September 11 terrorist attacks were of Arab origin, from Saudi Arabia, United Arab Emirates, Egypt, and Lebanon. Intelligence analysis could only have logically pointed the NYPD's Demographics Unit toward ethnic neighborhoods primarily occupied by Arab Americans, further obscured by neighborhoods occupied by Muslim Americans. Furthermore, while it may be inconvenient that the "faces of terrorism" are predominantly Arab, it does not change the fact that the faces are, in fact, Arab. The only way to mitigate the negative effects of these initiatives on the physical and mental well-being of Arab Americans is to work in concert with Arab Americans in combating terrorism. Similar to overseas efforts between the Departments of State and Defense and partner nations' counter-terrorism forces, the domestic law enforcement apparatus should work with Arab American community leaders in seeking to either apprehend or thwart would-be threats. Working with respected elements of Arab American society would likely allow law enforcement to operate more easily inside of ethnic communities without devoting the resources to covertly operate in the same communities. Mutual respect and the absence of institutional and/or individual prejudice is likely the only measure through which Arab or Muslim Americans will feel that they are on equal footing with their fellow citizens. Allied, the two groups could likely accomplish much more in the name of national security, they are, incidentally, all Americans. To that end, addressing domestic extremist groups will require the same combination of cultural sensitivity and local attention.

Notes

1. White House, *National Strategy for Counterterrorism* (Washington, DC: White House, 2011), https://www.hsdl.org/?view&did=487985.

2. Ibid, 8.

3. Ibid, 11.

4. White House, *Empowering Local Partners to Prevent Violent Extremism in the United States* (Washington, DC: White House, 2011), 1, https://www.hsdl.org/?view&did=682863.

5. U.S. Government Accountability Office, *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, GAO-17-300 (Washington, D.C., 2017), 28-34.

6. National Commission on Terrorist Attacks Upon the United States, *The 9-11 Commission Report* (Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004), 259, https://govinfo.library.unt.edu/911/report/911Report.pdf.

7. Missouri Information Analysis Center, *The Modern Militia Movement* (Jefferson City, MO: Missouri State Highway Patrol, 2009), https://thelastdemocrat.files.wordpress.com/2010/02/13290698-the-modern-militia-movementmissouri-miac-strategic-report-20feb09.pdf.

8. Office of the Director of National Intelligence, *Tearline Production and Dissemination*, IC Directive 209 (Washington, DC: Office of the Director of National Intelligence, 2012), https://www.odni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf.

9. U.S. Department of Homeland Security, *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment* (Washington, DC: Department of Homeland Security), 2, https://fas.org/irp/eprint/rightwing.pdf.

10. Ibid, 3.

11. Office of the Director of National Intelligence, *Sourcing Requirements for Disseminated Analytic Products*, IC Directive 206 (Washington, DC: Office of the Director of National Intelligence, 2015), https://www.dni.gov/files/documents/ICD/ICD%20206.pdf.

12. Office of the Director of National Intelligence, *Analytic Standards*, IC Directive 203 (Washington, DC: Office of the Director of National Intelligence, 2015), https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

13. Missouri Information Analysis Center, *The Modern Militia Movement*, 6.

14. U.S. Senate, Committee on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report: Permanent Subcommittee on Investigations*, 112th Cong., 1st sess., October 3, 2012, 104.

15. U.S. Department of Homeland Security, *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment*, 7.

16. David K. Rehbein to Janet Napolitano, April 13, 2009, in Fox News, https://www.foxnews.com/opinion/an-open-letter-to-homeland-security-on-rightwing-extremists.

17. Eli Lake and Audrey Hudson, "Napolitano Stands by Controversial Report," *Washington Times*, April 16, 2009, ProQuest.

18. Linton Weeks, "Museum Shooting Suspect Has Long Trail Of Vitriol," *NPR*, June 10, 2009, https://www.npr.org/templates/story/story.php?storyId=105223159.

19. "George Tiller Killed: Abortion Doctor Shot At Church," Huffington Post, July 1, 2009, https://www.huffpost.com/entry/george-tiller-killed-abor_n_209504.

20. R. Jeffrey Smith, "Homeland Security Department Curtails Home-grown Terror Analysis," *Washington Post*, June 7, 2011, ProQuest.

21. Ibid.

22. Lorenzo Vidino, *Countering Radicalization in America: Lessons from Europe*, Special Report 262 (Washington, DC: United States Institute of Peace, 2010), 2, https://www.usip.org/sites/default/files/resources/SR262%20-%20Countering_Radicalization_in_America.pdf.

23. Ibid, 6.

24. Homeland Security Advisory Council, *Countering Violent Extremism (CVE) Working Group* (Washington, DC: Department of Homeland Security, 2010), https://permanent.fdlp.gov/gpo20410/hsac-cve-working-group-recommendations.pdf.

25. White House, *Empowering Local Partners to Prevent Violent Extremism in the United States*, 5-6.

26. Ibid, 3.

27. Ibid, 5.

28. Ibid.

29. Dina Temple-Raston, "Somali-Americans Arrested In Islamic State Recruiting Plot," *NPR*, April 20, 2015, ProQuest.

30. U.S. Department of Homeland Security, "State and Major Urban Area Fusion Centers," 2012, https://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout_0.pdf.

31. "National Network of Fusion Centers," U.S. Department of Homeland Security, 2014, http://www.dhs.gov/national-network-fusion-centers-fact-sheet#1.

32. Brian Freskos, "Anti-Terror Agency Points to N.C. Case as Example of Success," *Star-News*, Feb 22, 2013, ProQuest.

33. Ibid.

34. Vanessa O'Connell, Stephanie Simon, and Evan Perez, "For the Love of Islam - A Second American Woman is Arrested in Cartoonist Case," *Wall Street Journal*, March 13, 2010, ProQuest.

35. Ibid.

36. "Demographics," Arab American Institute Foundation, 2018, https://assets.nationbuilder.com/aai/pages/9843/attachments/original/1551198642/National_Demographics_SubAncestries_2018.pdf.

37. Alixa Naff, "The Early Arab Immigrant Experience," in *The Development of Arab-American Identity*, ed. Ernest N. McCarus, (Ann Arbor: University of Michigan Press, 1994), 23.

38. Ibid.

39. Federal Bureau of Investigation, "Crime in the United States - 2001," Uniform Crime Reporting Program, 2002, https://ucr.fbi.gov/crime-in-the-u.s/2001.

40. Arab American Institute Foundation, *Profiling and Pride: Arab American Attitudes and Behavior Since September 11* (Washington, DC: Arab American Institute Foundation, 2003), ProQuest.

41. Wayne Baker, Ronald Stockton, Sally Howell, Amaney Jamal, Ann Chih Lin, Andrew Shryock, and Mark Tessler, *Detroit Arab American Study (DAAS) ICPSR04413-v2* (Ann Arbor, MI: Interuniversity Consortium for Political and Social Research [distributor], 2006), https://doi.org/10.3886/ICPSR04413.v2.

42. Ibid.

43. Ibid.

44. New York City Police Department, *Egyptian Locations of Interest Report* (New York: New York City Police Department, 2006), https://hosted.ap.org/specials/interactives/documents/nypd/nypd-egypt.pdf.

45. Adam Goldman and Matt Apuzzo, "Inside the Spy Unit That NYPD Says Doesn't Exist," *Associated Press*, August 31, 2011, ProQuest.

46. James McDermott to Robert Mueller, June 19, 2013, on the Representative James McDermott website, http://mcdermott.house.gov/images/pdf/facesterrorism.pdf.

47. Ibid.

48. Ronald C. Kessler, Kristin D. Mickelson, and David R. Williams, "The Prevalence, Distribution, and Mental Health Correlates of Perceived Discrimination in the United States," *Journal of Health and Social Behavior* 40, no. 3 (October 1999): 208-230, https://doi.org/10.2307/2676349.

49. Karmela Liebkind and Inga Jasinskaja-Lahti, "The Influence of Experiences of Discrimination on Psychological Stress: A Comparison of Seven Immigrant Groups," *Journal of Community & Applied Social Psychology 10*, no. 1 (2000): 1–16, https://doi.org/10.1002/(SICI)1099-1298(200001/02)10:1<1::AID-CASP521>3.0.CO;2-5.

50. Wahiba Abu-Ras and Soleman Abu-Bader, "The Impact of the September 11, 2001, Attacks on the Well-being of Arab Americans in New York City," *Journal of Muslim Mental Health 3*, no. 2 (2008): 217-239, https://doi.org/10.1080/15564900802487634.

51. Ibid, 221.

52. Ibid, 230.

53. John M. Venhaus, *Why Youth Join al-Qaeda*, Special Report 236, (Washington, DC: United States Institute of Peace, 2010), https://www.usip.org/publications/2010/05/why-youth-join-al-qaeda.

54. Ibid.

Chapter 2. Applying U.S. Power Smartly in East Africa: A Comparison of the Obama and Trump Administrations

National security and foreign policy are not mutually exclusive, neither are counterterrorism and diplomacy. The United States' counterterrorism strategy should exist as a component of a foreign policy that furthers U.S. interests through a whole-of-government effort without degrading its national institutions or international standing. To accomplish this, the United States must prioritize a "smart power" approach wherein military force is viewed as the exception instead of the rule and applied selectively for specific operations. This paper examines the United States' activities in East Africa during the Obama Administration, specifically efforts to counter the violent extremist organizations (VEO) al-Qaeda and al-Shabaab in Somalia. Acknowledging the value of metrics detailing tactical successes and appropriated foreign aid, this paper also assigns importance to the tone and consistency of administrations' public statements. Presidents are responsible for explaining strategy to the public, providing a rationale, and reporting successes or failures. An administration's public dialogue provides a context by which an international audience understands the United States' intentions, far beyond the text of a *National Security Strategy*. By comparing two diametrically different administrations' approaches, this paper ultimately seeks to identify an ideal model for U.S. counterterrorism policy outside of areas undergoing armed conflict.*

* The International Committee of the Red Cross defines "armed conflict" as either: international armed conflicts between two or more States; or, non-international armed conflicts whereby protracted armed confrontations occur within a State between governmental armed forces and the forces of one or more armed groups.

Power

Originally coined by Joseph S. Nye, "soft power" is "the ability to affect others to obtain the outcomes one wants through attraction rather than coercion or payment."[1] In states, according to Nye, this ability is tied to their "culture, values, and legitimate policies."[2] By contrast, "hard power" is a "carrots and sticks" approach whereby a state exercises military or economic measures to achieve its goals. The Department of Defense defines terrorism as "the unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political."[3] Although its practitioners most often belong to organized groups which can form alliances or even control territory, terrorism is a tactic. A counterterrorism policy that primarily consists of "hard power" military or cyber actions against VEOs without regard to societal realities that enable these groups' existence undermines any opportunity for lasting effects. Furthermore, members of VEOs typically live amongst the populations of states with whom the United States is not at war. While threats to U.S. interests and those of its allies, these entities exist in what Nadia Schadlow refers to as "the space between peace and war."[4†] A "soft power" projection of the United States' culture and values is unlikely to affect the groupthink that pervades many VEOs, especially those for which a rejection of modernity is a significant ideological plank. Here, Nye asserts the need for "smart power," an integrated strategy underscoring the "necessity of a strong military" with heavy investment in "alliances, partnerships, and institutions at all levels" to expand the United States' influence and legitimize its actions.[5] In a 2009 defense of "smart power", Nye pointed to disparate soft power capabilities

† The United States Special Operations Command (USSOCOM) refers to this as a "grey zone" security challenge, defined as "competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality."

throughout the U.S. government and the absence of a single policy integrating them with hard power capabilities.[6] The Obama Administration's arrival coincided with normalization of the term "3D" (defense, diplomacy, and development) to describe a balanced application of U.S. instruments of power.[7]

Somalia and al-Shabaab

Somalia occupies a strategic location on the Horn of Africa along southern approaches to the Bab el-Mandeb Strait, a vital shipping hub that connects the Gulf of Aden to the south and the Red Sea to the north.[8] The United States began diplomatic relations with Somalia after its establishment in 1960, following the withdrawal of the United Kingdom and Italy.[9] A coup in 1969 replaced the democratic government with an authoritarian socialist regime ideologically and economically dependent on the Soviet Union.[10] Belete Belachew Yihun notes that Somali relations with neighboring Ethiopia during the 1960s centered primarily on Somalia's "irredentist agenda of establishing a Greater Somalia" by claiming Ethiopian territory and Ethiopia's efforts to defend its territorial sovereignty.[11] By 1977, this sentiment served as the driving force behind Somali military incursions into the Ogaden desert, an ethnically Somali province in southern Ethiopia. Raymond Garthoff credits the Carter Administration's unwillingness to follow-through on pledges to support the Somali government in this conflict with both furthering a regional war and worsening relations between the United States and the Soviet Union.[12] The Carter Administration's decision to avoid a Cold War proxy conflict in East Africa has merit. However, from the Somali perspective, the incident demonstrates an instance of the United States reneging on its promises.

Al-Shabaab owes its origins largely to Al-Ittihad Al-Islami (AIAI), a militant Salafi extremist group that sprang from a collection of Middle Eastern-educated Somali extremists

which sought to establish an Islamist emirate in Somalia during the 1990s.[13] After AIAI disbanded in 1997, al-Shabaab became the military wing of the Islamic Courts Union (ICU), a movement that emerged from within the Somali justice system with the aim of controlling Somalia which culminated in its control of the capital Mogadishu in June 2006.[14] Driven by fears that the ICU-controlled government would pose a threat to its predominantly Christian population, neighboring Ethiopia invaded Somalia in December 2006 to remove the ICU from power. While successful in its stated objective of eliminating the perceived threat by the ICU, the invasion was the catalyst for the youth movement formerly associated with AIAI diverging from its focus of operating purely within Somalia.[15] The ensuing instability led the United Nations (UN) Security Council to authorize UN support to the African Union Mission in Somalia (AMISOM).[16] Since its establishment in 2007, AMISOM's mandate has evolved to include assisting Somali security forces "reduce the threat posed by al-Shabaab."[17] The invasion provided a hybrid nationalist-Islamist movement that swelled al-Shabaab's ranks and caused what counterterrorism expert Rob Wise describes as the transformation "from a small, relatively unimportant part of a more moderate Islamic movement into the most powerful and radical armed faction in the country."[18] Since 2010, the United States has contributed over $2.5 billion to AMISOM and over $500 million in security assistance for Somali forces.[19]

With international, regional, and secular adversaries, al-Shabaab turned its focus outside of Somalia with an intent to "connect the horn of Africa jihad to the one led by al-Qaeda and its leader Sheikh Osama bin Laden."[20] Initially, bin Laden was hesitant to formally align with al-Shabaab. In his reply a request for formal ties by al-Shabaab leader Sheikh Ahmad Abdi Godane "Abu Zubair," bin Laden wrote that "it would be better for [al-Shabaab] to say that there is a relationship with [al-Qaeda] which is simply a brotherly Islamic connection and nothing more,"

as a formal alliance would bring negative attention to al-Shabaab and exacerbate the "immense poverty and malnutrition" in Somalia.[21] To aid Muslims in Somalia, bin Laden offered what equated to"soft power" assistance: the al-Qaeda leader would use his sermons to encourage "merchants in the countries of the Arabian Peninsula to support pro-active and important developmental projects which are not expensive."[22] Al-Qaeda would not publicly acknowledge its alliance with al-Shabaab until 2012. Beyond its contributions toward Somalia's destabilization, al-Shabaab's entreaties to al-Qaeda and demonstrated ability to export terrorism with the 2013 attack on a shopping mall in Nairobi made the organization a threat to regional stability and therefore a more direct focus of U.S. security policy.

The Obama Administration

As a presidential candidate, then-Senator Barack Obama called for a "smart power" counterterrorism strategy of military action balanced against access to education, health care, trade, and investment, enabled and executed multilaterally.[23] National security and counterterrorism strategy during the Obama Administration's first term would reflect these sentiments, ultimately culminating in what would become known as the Obama Doctrine.[24] Announced in May 2014 at the United States Military Academy, the Obama Doctrine contained four pillars: a willingness to use unilateral military force to defend the United States or its allies; a commitment to counterterrorism; an effort to strengthen and enforce international order; and, a willingness to act on behalf of human dignity.[25] Citing the decentralized nature of al-Qaeda and its global affiliates, President Obama deemed U.S. military intervention in every country that harbors terrorists to be "naïve and unsustainable" and pointed to a need to "more effectively partner with countries where terrorist networks seek a foothold."[26] The 2010 *National Security Strategy* points to al-Qaeda's attempts to establish safe havens in at-risk states such as Somalia

as rationale for increased U.S. efforts to counter threats emanating from these countries.[27] The 2011 *National Strategy for Counterterrorism* cites al-Shabaab as the cause of "persistent instability and disorder" in Somalia that has allowed for an introduction of al-Qaeda elements into East Africa.[28] While the strategy distinguishes al-Qaeda as the United States' primary focus with respect to counterterrorism, the linkage between al-Qaeda and al-Shabaab provides a justification for the latter becoming a focus of U.S. counterterrorism efforts.

Citing the need to counter the narrative of al-Qaeda and its affiliates, President Obama created the Center for Strategic Counterterrorism Communications (CSCC) within the State Department.[29] CSCC was responsible for coordinating and informing the U.S. government's communications strategy against terrorism and violent extremism, as well as countering terrorist propaganda and misinformation about the United States by engaging in foreign languages on digital platforms commonly used by terrorists.[30] This method of "digital diplomacy," interagency staff, and relationship with the U.S. Intelligence Community (IC) represent an ideal "smart power" whole-of-government approach to counterterrorism; the CSCC's endurance is a testament to its success. In 2016, the CSCC was retitled the Global Engagement Center (GEC) and given broader authority to coordinate and synchronize counterterrorism messaging under a newly established Special Envoy and Coordinator for Global Engagement Communications.[31]

The U.S. Agency for International Development (USAID) leads the U.S. government's international development and disaster assistance efforts through partnerships and investments. USAID's familiarity with- and proximity to areas susceptible to community or individual radicalization make it uniquely suited to factor CVE into its mission. Since its 2011 partnership with Somalia, USAID has furthered U.S. CVE initiatives through programs aimed at strengthening civil society, increasing CVE and radicalization awareness, youth empowerment,

and good governance.[32] The agency's primary effort to reduce the potential for al-Shabaab influence is the Transition Initiatives for Somalia Plus (TIS+) program to increase political and social inclusion of marginalized populations, enable community reconciliation, and expand Somali government presence in areas formerly occupied by al-Shabaab.[33] Since 2015, TIS+ has funded projects to improve roads, repair municipal buildings, build airstrips, sponsor sporting events, and feed victims and first-responders after an al-Shabaab attack.[34] All of this is in accordance with priorities established by the National Security Strategy, but conducted by public representatives of the United States, absent a direct association with its "hard power" elements. Exclusive of foreign aid, the Obama Administration established the President's Advisory Council on Doing Business in Africa (PAC-DBIA) in 2014 to develop mutually beneficial trade opportunities between the United States and Africa, spanning public and private sectors.[35] To date, much of the PAC-DBIA's work has focused on outlining best practices for U.S. companies on approaching African markets and recommendations to mitigate risk. Recommendations for East Africa have been limited to Ethiopia and Kenya.[36] Finally, the Obama Administration launched Power Africa in 2013 as a multilateral initiative led by the U.S. government and coordinated by USAID that works to increase access to electricity in sub-Saharan Africa.[37] To date, Power Africa has enabled 16 million new connections to homes and businesses throughout forty countries.[38]

With al-Shabaab's violent response to AMISOM and pivot toward external attacks came the United States' March 2008 designation of the group as a Foreign Terrorist Organization (FTO) and its May 2008 targeted airstrike of Aden Hashi Ayro, the group's leader.[39] The Obama Administration cited the 2001 Authorization for the Use of Military Force (2001 AUMF) as its domestic legal basis for military actions (to include airstrikes) in Somalia targeting al-Qaeda and

al-Shabaab.[40] The administration's application of the 2001 AUMF was similar to the 2011 *National Strategy for Counterterrorism* language in that "associated forces" could be targeted by meeting two conditions: that it be "an organized, armed group that has entered the fight alongside al-Qa'ida or the Taliban," and that it be a "co-belligerent with al-Qa'ida or the Taliban in hostilities against the United States or its coalition partners."[41] While applying the same domestic legal basis that covered U.S. military operations in Afghanistan, the Bush and Obama Administrations' application of military force in Somalia relied primarily direct action (DA) by special operations forces (SOF).‡ Scholarly assessments of this approach's long-term efficacy are mixed, specifically with respect to airstrikes from unmanned aerial vehicles (UAV), but there is general agreement that DA against high-value individuals and non-Somali al-Qaeda members resented by the local civilian population had an overall weakening effect on al-Shabaab.[42]

The dynamic nature of areas in which DA is applied requires consideration of the potential second- and third-order effects of an operation. Tactical successes in Somalia by U.S. SOF would often come at the expense of AMISOM; a "guilt by association" in the eyes and minds of the civilian population that could lend itself al-Shabaab propaganda to foster public support. Mitigating this to some extent, the United States established a military coordination cell within AMISOM in 2013 to provide "planning and advisory support."[43] The external significance of maintaining a physical presence within AMISOM cannot be understated because it represents a degree of U.S. ownership over a shared problem, beyond funding. Internal to U.S. policy, a military presence within AMISOM represented a critical first step in linking the United States' tactical counterterrorism policy to its larger regional policy. Also in the realm of coercive

‡ In Joint Publication 3-05, *Special Operations* (2014), the Department of Defense defines direct action as "short-duration strikes and other small-scale offensive actions conducted as a special operation in hostile, denied, or diplomatically sensitive environments and which employ specialized military capabilities to seize, destroy, capture, exploit, recover or damage designated targets."

"hard power," President Obama first issued Executive Order (EO) 13536 of April 12, 2010, "Blocking Certain Persons Contributing to the Conflict in Somalia" to freeze assets of al-Shabaab in the United States, citing the group's role in destabilizing Somalia and enabling acts of piracy off its coast.[44] These sanctions would be expanded throughout the remainder of the Obama Administration and continued during the Trump Administration.

Congress

In Section 1287 of the 2017 National Defense Authorization Act (2017 NDAA), Congress expanded the GEC's mandate beyond counterterrorism by assigning it responsibility for countering "foreign state and non-state propaganda and disinformation efforts" that threaten U.S. national security.[45] This measure is effectively an inclusion of the Countering Foreign Propaganda and Disinformation Act of 2016, which called for a whole-of-government mechanism to counter foreign disinformation primarily from Russia and China.[46] As demonstrated by Russian activities during the 2016 U.S. presidential election and reports that the IC expects similar efforts in the 2020 elections, there is certainly a need to provide a counter-narrative to disinformation.[47] However, the statutory changes to the GEC omit any reference to counterterrorism or violent extremism, seemingly making these foci implied tasks.

In its report accompanying the 2017 NDAA, the House Armed Services Committee acknowledged successful messaging and propaganda campaigns by the Islamic State of Iraq and the Levant (ISIL) as indicative of a need for strategies to develop "regional counter-narrative capabilities" and to counter "adversarial messaging."[48] The committee's directives to the Secretary of Defense to develop strategies on these topics contained descriptions of CSCC and GEC core-functions, as outlined by President Obama in EO 13721, dated less that sixty days prior to the committee's report.[49] Bizarrely, the section of the House report entitled "Countering

Adversarial Messaging" is followed by a section entitled "Counterterrorism and Security Cooperation Efforts in Somalia and the Horn of Africa." The latter section commends the Defense Department's bilateral counterterrorism efforts against al-Shabaab, acknowledges the importance of a whole-of-government approach to security and stability in Somalia, and encourages the Departments of Defense and State to "continue coordination of efforts."[50]

President Obama requested that Congress fund a $5 billion Counterterrorism Partnerships Fund (CTPF) with which the United States would "train, build capacity, and facilitate partner countries" in Yemen, Somalia, Libya, and Mali.[51] In its proposal to Congress, the Obama Administration portioned $4 billion to the Department of Defense to "enhance its counterterrorism and crisis response activities," support foreign security forces, and fund enabling activities such as intelligence, transportation, and logistics.[52] Congress ultimately authorized $1.8 billion, allocating it from Overseas Contingency Operations (OCO) funds. Federal funding under OCO provides for the costs of deployed U.S. Armed Forces (pay, allowances, subsistence, and personnel costs) and associated operations and maintenance costs.

Congress's apparent missteps may be attributable to a modern favoring executive primacy over national security issues. Alexis de Tocqueville observed that executive weakness in the United States stemmed from an absence of foreign relations, suggesting that if the nation were "perpetually threatened (or) if its chief interests were in daily connection with those of other powerful nations," the President's "increased importance" would allow for the exercise of "almost royal prerogatives" already in his possession.[53] Applying de Tocqueville's logic to the United States' evolution into a superpower and its global presence aids in understanding the present-day imbalance favoring the President in national security matters.

With respect to congressional influence in foreign policy and war powers, James Lindsay suggests that Congress is reticent to leverage influence over appropriations involving military operations because it places Members in a "politically and morally difficult" position of reducing funding "to troops who may be fighting or their lives."[54] While not factually applicable to the CTPF funds, one could make a rhetorical case against the use of OCO funds allocated to combat operations in Afghanistan, Iraq, and Syria being used for an initiative that could be categorized as foreign aid. Taken together, Congress's placement of CTPF funds in OCO and its directive to the Secretary of Defense to develop a strategy duplicating the GEC's efforts indicates an inclination to reflexively leverage the military against a counterterrorism problem. A "whole-of-government" approach must include an informed Congress.

The Trump Administration

The Trump Administration's 2017 *National Security Strategy* prioritizes competition with China and Russia and countering the Democratic People's Republic of Korea and the Islamic Republic of Iran above counterterrorism.[55] The strategy contains no mention of Somalia or al-Shabaab, and characterizes Africa as being home to "potential new markets for U.S. good and services."[56] Similarly, its 2018 *National Strategy for Counterterrorism* contains no mention of Somalia or al-Shabaab; the single mention of Africa is part of a generalized statement concerning the Islamic State of Iraq and al-Sham (ISIS).[57] Then-National Security Advisor John R. Bolton outlined the administration's three core interests in Africa: advancing U.S. trade and commercial ties; countering "radical Islamic terrorism;" and, efficient and effective U.S. aid that will advance U.S. interests.[58] In early 2017, the Department of Defense announced presidential approval of its proposal support AMISOM and Somali security forces with "additional precision fires" on the same day that the *New York Times* reported that President Trump had declared

portions of Somalia an "area of active hostilities."[59] The administration's increase in airstrikes (thirty-four in 2017 and forty-one in 2018) eclipsed those authorized during the two previous administrations.

Table 1. Total Strikes and Fatality Estimates[60]

Administration	Strikes	Deaths			
	Total	Civilians	Unknown	Militants	Total
Bush	12	26 – 68	13 – 21	38 – 55	77 – 144
Obama	48	1 – 22	10	338 – 521	349 – 553
Trump	187	7 – 23	33 – 37	987 – 1,085	1,027 – 1,145
Total	**247**	**34 – 113**	**56 – 68**	**1,363 – 1,661**	**1,453 – 1,842**

The exponential increase of airstrikes in Somalia from 2017 to 2020 has been complemented by Trump Administration budget proposals requesting significant cuts to the Department of State, USAID, and the CTPF program.[61] Strategies vary over administrations and are driven by policies that are influenced by changing events and worldviews. There is no public expectation that one administration will adopt policies or strategies of its predecessor; merely that national strategy in each area progresses toward an ideal. The Trump Administration's treatment of its stated core interests in Africa as mutually exclusive disregards any historical context that could be gained from the United States' experience in East Africa.

Aside from military operations, the cornerstone of the Trump Administration's Africa policy is the Prosper Africa initiative. Prosper Africa seeks to increase two-way trade and investment between the United States and African countries by providing prospective investors with "tool kits" to leverage U.S. government resources that will enable "deals."[62] The initiative builds upon existing programs such as Power Africa and those authorized by the African Growth and Opportunity Act.[63] Although Prosper Africa does not create new programs, it provides a central location in which interested parties can navigate U.S. government policies with respect to

African markets, making it useful for private sector entities lacking a familiarity with the minutia of U.S. import-export regulations. As the United States endeavors to counter China's Belt and Road Initiative (BRI) in Africa, it will be critical to offer African nations an expansive palate of alternatives to otherwise enticing entreaties of Chinese development projects. However, as former USAID Administrator Andrew S. Nastios notes, "the international development space abhors a vacuum."[64] The PAC-DBIA's warnings of risk for private investment reflect potential hesitation on the part of private sector investment.[65] Progress in development cannot be accomplished without societal stability in the places in need of development. The Trump Administration's annual proposed budget cuts to foreign aid, the State Department, and USAID by, on average, twenty percent, likely stall regional stability – and by extension, its Prosper Africa initiative.

Despite military or economic gains made during the Trump Administration, the President's public comments about Somalia and its diaspora in the United States likely cast a shadow over any progress made by its policies. Three episodes likely degrade regional confidence in the United States. First, seven days after his 2017 inauguration, President Trump issued EO 13769, suspending immigration to the United States from Somalia and six other Muslim-majority countries on national security grounds, citing the possibility that terrorists could enter the United States whilst acting as refugees.[66] After legal challenges, EO 13769 was revoked and replaced by EO 13780, which reasserted the suspension of immigration from Somalia and five countries on similar grounds.[67] While EO 13780 acknowledged Somalia's cooperation with the United States on "some counterterrorism operations," it cited the Somali government's lack of capacity to "sustain military pressure on or to investigate suspected terrorists" as a rationale to end immigration from Somalia.[68] Second, press accounts in 2018

detailed a White House meeting about immigration with Members of Congress in which President Trump reportedly referred to Haiti, El Salvador, and African countries as "shithole countries."[69] As the White House disputed these reports without explicitly denying them, statements of concern and condemnation were released by the UN, African Union, and editorialized throughout Africa.[70] Finally, President Trump spent much of 2019 attacking Somali-born Representative Ilhan Omar (D-MN) in public statements and social media with accusations of anti-Semitism, suggesting the Congresswoman and three other minority Congresswomen should "go back and help fix the totally broken and crime infested places from which they came."[71] During campaign rallies in North Carolina and Minnesota, the President oversaw crowds chanting "send her back" and criticized the Minneapolis mayor for allowing Somali refugees to settle in the city, while touting a presidential proclamation from the previous month that suspended all immigration from Somalia and required additional scrutiny on visa adjudications for Somali nationals.[72] Reflecting on the evolution of presidents as international leaders following WWII, Richard P. Longaker advises that presidents not permit the quality of international leadership to be guided by aspirations for domestic popularity, as this could "cast doubt on his capacity to lead abroad."[73] Although Somali institutional weaknesses were referenced in EOs 13769 and 13780, their inclusion was likely a nod to the President's domestic political narrative on immigration reform rather than an aspect of a larger counterterrorism strategy.

Conclusion

Nye asserts that contextual intelligence is the key to producing a "smart power" strategy.[74] As relations between the United States and Soviet Union were deteriorating during the Ogaden conflict on the Horn of Africa, China quietly maintained positive relations with both

Somalia and Ethiopia.[75] This should be instructive to U.S. policymakers as they rank counterterrorism lower among the United States' national security priorities in the era of great power competition. If U.S. foreign policy in Somalia emphasizes aid, development, good governance, security assistance, and low intensity counterterrorism operations, the outcome could be a favorable regional view of the United States by nations considering partnership with China. None of this can be accomplished without mutual trust; recipients of U.S. foreign aid should not be characterized by an administration as burdensome to the American taxpayer. As the Chief Executive of the United States and its chief policymaker, responsibility falls to the President to craft a "smart" foreign policy capable of achieving its stated goals and messaging it domestically and internationally with a tone of empathy that reflects American ideals.

Notes

1. Joseph S. Nye, "Public Diplomacy and Soft Power," *The Annals of the American Academy of Political and Social Science* 616 (2008): 94-109, JSTOR.

2. Diane Coutou, "Smart Power," *Harvard Business Review*, November 2008, https://hbr.org/2008/11/smart-power/.

3. Joint Chiefs of Staff, *Antiterrorism*, JP 3-07.2 (Washington, DC: Joint Chiefs of Staff, 2010), https://www.hsdl.org/?view&did=753152; see also Antiterrorism Act of 1990, 18 U.S.C. § 2331 (2018), https://www.law.cornell.edu/uscode/text/18/2331.

4. Nadia Schadlow, "Peace and War: The Space Between," *War on the Rocks* (blog), August 18, 2014, https://warontherocks.com/2014/08/peace-and-war-the-space-between/; U.S. Special Operations Command, *The Grey Zone* (Tampa, FL: USSOCOM, 2015), https://www.soc.mil/swcs/ProjectGray/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf.

5. CSIS Commission on Smart Power, *CSIS Commission on Smart Power: A Smarter, More Secure America*, (Washington, DC: CSIS, 2007), https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/071106_csissmartpowerreport.pdf.

6. Joseph S. Nye, "Get Smart: Combining Hard and Soft Power," *Foreign Affairs*, July-August 2009, https://www.foreignaffairs.com/articles/2009-07-01/get-smart.

7. Nathan Finney, "A Culture of Inclusion: Defense, Diplomacy, and Development as a Modern American Foreign Policy," *Small Wars Journal* (blog), September 26, 2010, https://smallwarsjournal.com/blog/journal/docs-temp/553-finney.pdf.

8. “Somalia,” Central Intelligence Agency, June 17, 2020, https://www.cia.gov/library/publications/the-world-factbook/geos/so.html.

9. “U.S. Relations With Somalia: Bilateral Relations Fact Sheet," Department of State, 2019, https://www.state.gov/u-s-relations-with-somalia/.

10. Department of State, “U.S. Relations With Somalia: Bilateral Relations Fact Sheet.”

11. Belete Belachew Yihun, "Ethiopian Foreign Policy and the Ogaden War: The Shift From 'Containment' to 'Destabilization,' 1977-1991," *Journal of Eastern African Studies* 8, no. 4 (2014): 677, https://doi.org/10.1080/17531055.2014.947469.

12. Raymond Garthoff, *Détente and Confrontation: American-Soviet Relations from Nixon to Reagan*, rev. ed. (Washington, DC: Brookings, 1994), 695.

13. Clarie Felter, Jonathan Masters, and Mohammed Aly Sergie, "Al-Shabab," Council on Foreign Relations, last modified January 10, 2020, https://www.cfr.org/backgrounder/al-shabab.

14. "Al Shabaab," Stanford University, January 2019, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/al-shabaab; Felter, Masters, and Sergie, "Al-Shabab."

15. Felter, Masters, and Sergie, "Al-Shabab."

16. Security Council resolution 1744, The situation in Somalia, S/RES/1744 (2007) (20 February 2007).

17. Security Council resolution 1744, AMISOM, S/RES/2742 (2019) (31 May 2019).

18. Rob Wise, *Al Shabaab*, (Washington, DC: CSIS 2011), https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/110715_Wise_AlShabaab_AQAM%20Futures%20Case%20Study_WEB.pdf.

19. U.S. Library of Congress, Congressional Research Service, *Somalia*, by Lauren Ploch Blanchard, IF10155 (2020).

20. Felter, Masters, and Sergie, "Al-Shabab."

21. Usama bin Laden to Mukhtar Abu al-Zubayr, August 7, 2010, in Combating Terrorism Center at West Point, https://ctc.usma.edu/wp-content/uploads/2013/10/Letter-from-Usama-Bin-Laden-to-Mukhtar-Abu-al-Zubayr-Trnaslation.pdf.

22. Ibid.

23. Barack Obama, "Renewing American Leadership," *Foreign Affairs*, July-August 2007, https://www.foreignaffairs.com/articles/2007-07-01/renewing-american-leadership.

24. White House, *National Security Strategy* (Washington, DC: White House, 2010), http://nssarchive.us/national-security-strategy-2010/; White House, *National Strategy for Counterterrorism* (Washington, DC: White House, 2011), https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf; White House, *U.S. Strategy Toward Sub-Saharan Africa* (Washington, DC: White House, 2012), https://www.hsdl.org/?view&did=712667.

25. "Remarks by the President at the United States Military Academy Commencement Ceremony," West Point, New York, May 28, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/05/28/remarks-president-united-states-military-academy-commencement-ceremony.

26. Ibid.

27. White House, *National Security Strategy*, 21.

28. White House, *National Strategy for Counterterrorism*, 14.

29. "Executive Order 13584 of September 9, 2011, Developing an Integrated Strategic Counterterrorism Communications Initiative and Establishing a Temporary Organization to Support Certain Government-wide Communications Activities Directed Abroad," *Federal Register* 76, no. 179 (September 15, 2011): 56945-56947, https://www.govinfo.gov/content/pkg/FR-2011-09-15/pdf/2011-23891.pdf.

30. "Center for Strategic Counterterrorism Communications," Department of State, 2011, https://2009-2017.state.gov/documents/organization/116709.pdf.

31. "Executive Order 13721 of March 14, 2016, Developing an Integrated Global Engagement Center to Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584," *Federal Register* 81, no. 52 (March 17, 2016): 14685-14688, https://www.govinfo.gov/content/pkg/FR-2016-03-17/pdf/2016-06250.pdf.

32. "Countering Violent Extremism in Kenya, Somalia, and East Africa," U.S. Agency for International Development, 2019, https://www.usaid.gov/sites/default/files/documents/1860/Countering_Violent_Extremism_fact_sheet_February_2019.pdf

33. "Transition Initiatives for Stabilization + (TIS+)," U.S. Agency for International Development, 2020, https://www.usaid.gov/sites/default/files/documents/1860/Fact-Sheet-Somalia-TISfeb-2020.pdf

34. "Transition Initiatives for Stabilization + (TIS+)," U.S. Agency for International Development, 2020.

35. "Executive Order 13675 of August 5, 2014, Establishing the President's Advisory Council on Doing Business in Africa," Federal Register 79, no. 153 (August 8, 2014): 46661-46663, https://www.govinfo.gov/content/pkg/FR-2014-08-08/pdf/2014-18998.pdf; "President's Advisory Council on Doing Business in Africa - Charter," U.S. Department of Commerce, 2020, https://legacy.trade.gov/pac-dbia/charter.asp.

36. President's Advisory Council on Doing Business in Africa, *Fact-Finding Trip Report and Recommendations* (Washington, DC: Department of Commerce, 2018), https://legacy.trade.gov/pac-dbia/docs/PAC-DBIA%20Final%20Report%20Sep%202018.pdf.

37. "Power Africa," U.S. Agency for International Development, 2020, https://www.usaid.gov/sites/default/files/documents/1860/PowerAfrica_Fact_Sheet06262020.pdf .

38. "Power Africa," U.S. Agency for International Development, 2020.

39. Foreign Terrorist Organizations," U.S. Department of State, 2020, https://www.state.gov/foreign-terrorist-organizations/; Stephanie McCrummen and Karen DeYoung, "U.S. Airstrike Kills Somali Accused of Links to Al-Qaeda," *Washington Post*, May 2, 2008, ProQuest.

40. White House, *Report on the Legal and Policy Frameworks Guiding the United States' Use of Military Force and Related National Security Operations*, (Washington, DC: White House, 2016), https://www.hsdl.org/?view&did=798033.

41. White House, *Report on the Legal and Policy Frameworks Guiding the United States' Use of Military Force and Related National Security Operations,* (2016) 4-5; Authorization for the Use of Military Force, 50 U.S.C. § 1541 (2001).

42. Bronwyn E. Bruton and Paul D. Williams, *Counterinsurgency in Somalia: Lessons Learned from the African Union Mission in Somalia, 2007-2013*, JSOU Report 14-5 (Tampa, FL: Joint Special Operations University, 2014), https://www.socom.mil/JSOU/JSOUPublications/JSOU14-5_BrutonWilliams_AMISOM_FINAL.pdf; Katherine Zimmerman, Jacqulyn Meyer Kantack, Colin Lahiff and Jordan Indermuehle, *US Counterterrorism Objectives in Somalia: Is Mission Failure Likely?* (Washington, DC: American Enterprise Institute, 2017), https://www.criticalthreats.org/wp-content/uploads/2017/03/US-Counterterrorism-Objectives-in-Somalia.pdf.

43. David S. Cloud, "U.S. Military Secretly Sent Small Team of Advisors to Somalia," *Los Angeles Times*, January 10, 2014, https://www.latimes.com/world/worldnow/la-fg-wn-somalia-us-military-advisers-20140110-story.html; Bruton and Williams, *Counterinsurgency in Somalia: Lessons Learned from the African Union Mission in Somalia, 2007-2013*, 81.

44. "Executive Order 13536 of April 12, 2010, Blocking Certain Persons Contributing to the Conflict in Somalia," *Federal Register* 75, no. 72 (April 15, 2010): 19869-19872, https://www.govinfo.gov/content/pkg/FR-2010-04-15/pdf/2010-8878.pdf; "Executive Order 13620 of July 20, 2012, Taking Additional Steps to Address the National Emergency With Respect to Somalia," *Federal Register* 77, no. 142 (July 24, 2010): 43483-43485, https://www.govinfo.gov/content/pkg/FR-2012-07-24/pdf/2012-18237.pdf.

45. National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114–328, 130 Stat. 2546 (2016), https://uscode.house.gov/statviewer.htm?volume=130&page=2546.

46. Countering Foreign Propaganda and Disinformation Act of 2016, H.R. 5181, 114th Cong., 2d sess. (May 10, 2016), https://www.congress.gov/bill/114th-congress/house-bill/5181.

47. Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, (Washington, DC: National Intelligence Council, 2016), https://www.dni.gov/files/documents/ICA_2017_01.pdf; Ellen Nakashima, Shane Harris, Josh

Dawsey, and Anne Gearan, "Senior Intelligence Official Told Lawmakers that Russia Wants to See Trump Reelected," *Washington Post*, February 21, 2020, ProQuest.

48. U.S. House of Representatives, Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2017: Report (to Accompany H.R. 4909)*, 114th Cong., 2d. sess., 2016, H. Rept. 114-537, 241-247, https://www.congress.gov/114/crpt/hrpt537/CRPT-114hrpt537.pdf.

49. U.S. House of Representatives, Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2017: Report (to Accompany H.R. 4909)*, 241.

50. U.S. House of Representatives, Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2017: Report (to Accompany H.R. 4909)*, 241-242.

51. "Remarks by the President at the United States Military Academy Commencement Ceremony," West Point, New York, May 28, 2014.

52. Nina Serafino, *The Counterterrorism Partnerships Fund (CTPF) Proposal: Questions for Congress*, CRS Report No. IN10103 (Washington, DC: Congressional Research Service, 2014), https://fas.org/sgp/crs/terror/IN10103.html.

53. Alexis de Tocqueville, *On Democracy*, ed. Richard D. Heffner (New York: New American Library of World Literature, 1956), 80-81.

54. James M. Lindsay, *Congress and the Politics of U.S. Foreign Policy* (Baltimore: Johns Hopkins University Press, 1994), 151.

55. White House, *National Security Strategy* (Washington, DC: White House, 2017), http://nssarchive.us/national-security-strategy-2017/.

56. White House, *National Security Strategy*, 33.

57. White House, *National Strategy for Counterterrorism* (Washington, DC: White House, 2018), https://www.hsdl.org/?view&did=816990.

58. "Remarks by National Security Advisor Ambassador John R. Bolton on the The Trump Administration's New Africa Strategy," Washington, DC, December 12, 2018, https://www.whitehouse.gov/briefings-statements/remarks-national-security-advisor-ambassador-john-r-bolton-trump-administrations-new-africa-strategy/.

59. "Statement by Pentagon Spokesman Capt. Jeff Davis on U.S. Counterterrorism Operations in Somalia," Department of Defense press release, March 30, 2017, on the Department of Defense website, https://www.defense.gov/Newsroom/Releases/Release/Article/1135338/statement-by-pentagon-spokesman-capt-jeff-davis-on-us-counterterrorism-operatio/; Charlie Savage and Eric Schmidt, "Trump Eases Combat Rules in Somalia Intended to Protect Civilians," *New York Times*, March

30, 2017, ProQuest; Jason Burke, "Trump's Offensive to 'Wipe Out' al-Shabaab Threatens More Pain for Somalis," *The Guardian*, April 22, 2017, https://www.theguardian.com/world/2017/apr/22/us-action-al-shabaab-somalia-millions-famine-drought.

60. "The War in Somalia," New America, July 21, 2020, https://www.newamerica.org/international-security/reports/americas-counterterrorism-wars/the-war-in-somalia/.

61. White House, *America First: A Budget Blueprint to Make America Great Again, Budget of the United States Government, Fiscal Year 2018* (Washington, DC: Office of Management and Budget, 2017), https://www.govinfo.gov/content/pkg/BUDGET-2018-BUD/pdf/BUDGET-2018-BUD.pdf; White House, *Budget of the United States Government, Fiscal Year 2019* (Washington, DC: Office of Management and Budget, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf; White House, *Budget of the United States Government, Fiscal Year 2021* (Washington, DC: White House, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/02/budget_fy21.pdf; White House, *Budget of the United States Government, Fiscal Year 2020* (Washington, DC: White House, 2019), https://www.govinfo.gov/content/pkg/BUDGET-2020-BUD/pdf/BUDGET-2020-BUD.pdf.

62. "Prosper Africa Toolkit: U.S. Government Trade and Investment Services," U.S. Department of Commerce, 2020, https://legacy.trade.gov/prosperafrica/usgtools.pdf.

63. Trade and Development Act, 19 U.S.C. § 3701 (2001); African Growth and Opportunity Act, 19 U.S.C. § 3701 (2015).

64. Andrew S. Nastios, "Foreign Aid in an Era of Great Power Competition," *PRISM* 8, no. 4 (2020): 107.

65. President's Advisory Council on Doing Business in Africa, *Fact-Finding Trip Report and Recommendations* (Washington, DC: Department of Commerce, 2018), https://legacy.trade.gov/pac-dbia/docs/PAC-DBIA%20Final%20Report%20Sep%202018.pdf.

66. "Executive Order 13769 of January 27, 2017, Protecting the Nation From Foreign Terrorist Entry Into the United States," *Federal Register* 82, no. 20 (February 1, 2017): 8977-8982, https://www.govinfo.gov/content/pkg/FR-2017-02-01/pdf/2017-02281.pdf.

67. "Executive Order 13780 of March 6, 2017, Protecting the Nation From Foreign Terrorist Entry Into the United States," *Federal Register* 82, no. 45 (March 9, 2017): 13209-13219, https://www.govinfo.gov/content/pkg/FR-2017-03-09/pdf/2017-04837.pdf.

68. Ibid.

69. Julie Hirschfled Davis, Sheryl Gay Stolberg, and Thomas Kaplan, "Trump Alarms Lawmakers With Disparaging Words for Haiti and Africa," *New York Times*, January 11, 2018,

ProQuest; Josh Dawsey, "Trump Derides Protections for Immigrants from 'Shithole' Countries," *Washington Post*, January 12, 2018, ProQuest.

70. Eli Rosenberg and Paul Schemm, "'Here is What my #shithole Looks Like': African Countries and Haiti React to Trump's Remark," *Washington Post*, January 12, 2018, ProQuest; "Press Briefing by Press Secretary Sarah Sanders and Dr Ronny Jackson," White House, January 16, 2018, https://www.whitehouse.gov/briefings-statements/press-briefing-by-press-secretary-sarah-sanders-and-dr-ronny-jackson-01162018/; "Press Briefing by Press Secretary Sarah Sanders," White House, January 23, 2018, https://www.whitehouse.gov/briefings-statements/press-briefing-press-secretary-sarah-sanders-012318/.

71. Donald J. Trump (@realDonaldTrump), "What's completely unacceptable is for Congesswoman Omar to target Jews, in this case Stephen Miller." Jeff Ballabon, B2 Strategic, CEO." Twitter, April 9, 2019, 11:36 a.m., https://twitter.com/realDonaldTrump/status/1115639577102962691?s=20; Donald J. Trump (@realDonaldTrump), "Representatives Omar and Tlaib are the face of the Democrat Party, and they HATE Israel!" Twitter, August 15, 2019, 12:38 p.m., https://twitter.com/realDonaldTrump/status/1162040855328436225?s=20; Donald J. Trump (@realDonaldTrump), "It would show great weakness if Israel allowed Rep. Omar and Rep.Tlaib to visit. They hate Israel & all Jewish people, & there is nothing that can be said or done," Twitter, August 15, 2019, 9:57 a.m., https://twitter.com/realDonaldTrump/status/1162000480681287683?s=20.

72. Meagan Flynn, 'Malignant, Dangerous, Violent': Trump Rally's 'Send her Back!' Chant Raises New Concerns of Intolerance," *Washington Post*, July 18, 2019, ProQuest; "President Trump Campaign Rally in Minneapolis," Minneapolis, Minnesota, October 10, 2019, https://www.c-span.org/video/?464823-1/president-trump-holds-rally-minneapolis-minnesota&start=5599; U.S. President, Proclamation, "Enhancing Vetting Capabilities and Processes for Detecting Attempted Entry Into the United States by Terrorists or Other Public-Safety Threats, Proclamation 9645 of September 24, 2017," *Federal Register* 82, no. 186 (September 27, 2017): 45161-45172, https://www.govinfo.gov/content/pkg/FR-2017-09-27/pdf/2017-20899.pdf.

73. Richard P. Longaker, "The President as International Leader," *Law and Contemporary Problems* 21, no. 4 (Autumn 1956): 752, doi:10.2307/1190193.

74. Joseph S. Nye, "Get Smart: Combining Hard and Soft Power," *Foreign Affairs*.

75. Raymond Garthoff, *Détente and Confrontation: American-Soviet Relations from Nixon to Reagan*, 718.

Chapter 3: Cybersecurity as an Aspect of Smart Counterterrorism Policy

The United States' collective reliance on the Internet demands an in-kind investment in its security. The U.S. government must acknowledge its responsibility for national cybersecurity by immediately laying the groundwork to implement reforms recommended by the U.S. Cyberspace Solarium Commission ("The Commission") to achieve a new strategic approach to cybersecurity through layered cyber deterrence. The Commission's final report contains over eighty recommendations organized into six pillars: Reform the U.S. Government's Structure and Organization for Cyberspace; Strengthen Norms and Non-Military Tools; Promote National Resilience; Reshape the Cyber Ecosystem; Operationalize Cybersecurity Collaboration with the Private Sector; and, Preserve and Employ the Military Instrument of National Power.[1] This chapter will discuss two of the Commission's recommendations: strengthen the Cybersecurity and Infrastructure Agency (CISA), and expand international engagement to strengthen and reinforce norms in cyberspace. The U.S. government's current piecemeal approach to cybersecurity pits an outdated organizational structure consisting of multiple departments, agencies, and oversight bodies against rapidly evolving threats; absent the strategic coherence required to ensure national defense. This chapter asserts that the United States should seek inspiration from British and Australian policy models to foster a culture change in which it considers cybersecurity differently; strategically. Such a shift in thought will enable the United States to both counter and respond to acts of cyberterrorism.*

* Drawing on several legal and academic definitions of "terrorism," Eric Luiijf defines "cyberterrorism" as: the use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organization; made for the purposes of advancing a political, religious, racial or ideological cause; and it involves or causes: violence to, suffering of, serious injuries to, or the death of (a)

Thinking Strategically

In a 2007 article in the *Harvard Business Review* titled "How to Think Strategically," Michael D. Watkins details several approaches for developing one's strategic thinking ability. Included is a recommendation to use "case-based education," on the basis that exposure to others' comparable events will allow one to recognize key distinctions that (hopefully) drive "significant differences in outcomes."[2] Simply put: considering what happened in past similar situations can drive us to make adjustments that will likely improve how we react and in-turn, the results. While the previous chapter's use of the Carter Administration provides an opportunity to see this theory in practice, this chapter offers an instance from U.S. military history to illustrate the point.

Prior to the outbreak of World War II, the British Royal Navy (RN) made significant gains in its prosecution of antisubmarine warfare, most notably the recognition that convoy systems were instrumental in protecting merchant shipping against German U-boat attacks. This experience influenced changes in RN doctrine, technology development, and organizational structure with respect to the flow of intelligence. In August 1940, the U.S. Navy began participating in the Bailey Committee, a British military committee consisting of senior officers formed for the purpose of overseeing Anglo-American cooperation at the strategic, operational, and tactical levels.[3] U.S. Navy personnel were granted an unprecedented level of access to sensitive British intelligence, RN personnel, facilities, and ships.[4] In spite of its officers' reports of effective doctrine citing this access and exposure, U.S. Navy leadership would not establish coastal convoys along the East Coast of the United States until May 1942, nor would it establish an overall Interlocking Convoy System until September 1942.[5] Quite simply, the U.S. Navy

---

persons(s); serious damage to a property; serious risk to the health and safety of the public; serious economic loss; serious breach of ecological safety; serious breach of the social and political stability and cohesion of a nation.

failed to learn in the face of demonstrable expertise. The U.S. Navy defined learning and readiness in technical terms, thus focusing on British technology and ship designs that could increase the size and technical efficacy of its fleet instead of the underlying doctrine that allowed the RN to effectively implement this technology.[6] In failing to update its doctrine and make complementary organizational changes, the U.S. Navy squandered time in which it could have better prepared for entry into World War II. The Royal Australian Navy (RAN) completed design of its *Bathurst* class minesweepers in 1939, the "Australian corvette" would become the RAN's ship of choice for escort operations.[7] Inspired by the RN, the RAN began implementing similar doctrinal and organizational changes in 1940, albeit with a larger margin for error in the Pacific than the U.S. Navy in the Atlantic, as the Japanese submarine threat was less advanced than that of German U-boats.[8] August 2020 will mark seventy years since U.S. Navy officers attended the Bailey Committee, and once again, the United States is able to learn from the United Kingdom.

Critical Infrastructure

The Critical Infrastructures Protection Act of 2001 defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[9] While this remains the official U.S. government definition, the Congressional Research Service notes that policymakers have "lowered the threshold of criticality to infrastructure-related events with disruptive, but not necessarily catastrophic" effects across society.[10] As such, policy "increasingly reflects local, society-centric perspectives on infrastructure that place emphasis on it as an enabler of prosperity, public safety, and civic life."[11]

On April 19, 1995, Timothy McVeigh detonated a bomb inside of a truck he had parked in front of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. In what the FBI classified as "the worst act of homegrown terrorism" in U.S. history, one hundred sixty-eight people were killed and several hundred were injured.[12] The incident caused the Clinton Administration to consider the likelihood and consequences of a similar attack against critical infrastructure facilities. Executive Order (EO) 13010 of July 15, 1996 established President's Commission on Critical Infrastructure Protection (PCIP) to aid in developing a strategy for protecting critical infrastructure from two categories of threats: physical and cyber.[13]

The PCIP final report focused primarily on cyber threats, painting a troubling portrait of the ease with which the United States could be brought to a standstill resulting from a cyber attack on the following sectors: information and communications; energy; banking and finance; physical distribution; and, vital human services.[14] To illustrate the point, PCIP likened the effects of a physical attack involving a "satchel of dynamite" or a "truckload of fertilizer and diesel fuel" to a cyber-attack that involving "the right command sent over a network."[15] The former is an immediate event that requires an attacker's proximity to a single facility, thereby allowing the government to mount a response and assign blame. In contrast, a cyber attacker's proximity is virtual, requiring only an Internet connection. Furthermore, PGIP noted the high unlikelihood that facilities could immediately detect an intrusion or even discover "that a concerted [cyber-attack] is in progress," and that it could take "months, even years" to accurately assess damage inflicted by a cyber-attack.[16]

As Chief of the National Security Council (NSC) Counterterrorism Security Group (CSG) under President Clinton, Richard A. Clarke recalled surprise within the administration that PGIP had focused so heavily on cyber threats to critical infrastructure as opposed to "right

wingers like [Timothy] McVeigh and [Terry] Nichols or al Qaeda terrorists who had attacked the World Trade Center in 1993."[17] Among its recommendations, PCIP stressed the importance of a partnership between government and private sector infrastructure owners and operators, stressing a need for "information sharing."[18] Assuming more broad responsibilities in the Clinton Administration with the job title "National Coordinator for Security, Infrastructure, Protection, and Counter-terrorism," Clarke recounts his realization that PCIP's characterization of the public-private relationship as a "partnership" was deliberate; designed to overcome private sector wariness as the prospect of being subject to government regulations in the name of cybersecurity.[19] While the recommendations contained in the PCIP report come nowhere near creating a collision between the private sector and government authority for the sake of national security on the scale of *Youngstown v. Sheet & Tube Co. v. Sawyer*, their significance lies in the fact that the report represents the first public U.S. government assertion requiring private sector participation to secure critical infrastructure.[20]

Two of the Five Eyes: The United Kingdom and Australia

With the prioritization of cybersecurity in its 2015 *National Security Strategy*, the British government released a comprehensive 2016 *National Cyber Security Strategy* instituting a government-driven effort to significantly improve its national cybersecurity.[21] To execute its strategy, the British government created a single, central, national-level body as its "authoritative voice" on cybersecurity: The National Cyber Security Centre (NCSC).[22] As the government's "strong public face," the NCSC leverages intelligence from the Government Communications Headquarters (GCHQ) to inform its three-prong mission: incident management capability to respond to and reduce the harm from cyber incidents; educate public and private sector organizations on cybersecurity issues; and, provide expert sectoral advice to government and

critical sectors like telecommunications, energy, and finance.[23†] The NCSC provides an organizational model by which the United States can clarify and strengthen CISA's role into the government's single focal point for public-private cybersecurity efforts.[24]

The Australian government employs an "all hazards" strategy toward critical infrastructure security that differentiates between *resilience* and *protection*.[25] While the latter describes "actions or measures undertaken to mitigate against the specific threat of terrorism" which are overseen by a separate government entity – the Australian and New Zealand Counter-Terrorism Committee (ANZCTC) – this is essentially a distinction without a difference, as the "all hazards" approach to resilience includes terrorism.[26] In 2017, the Australian government created the Critical Infrastructure Centre (CIC) to implement its strategy and to serve as a focal point for public-private cooperation, building public sector resiliency by assessing risk and providing advice.[27] As CIC is more or less identical to NCSC in form and function, it is no more of a model for the United States than the latter; CIC is exceptional because of its regulatory authority. CIC administers the Security of Critical Infrastructure Act 2018, which authorizes:

- A requirement that owners and operators of certain critical infrastructure assets register ownership and operational information with the government.
- The Secretary of the Department of Home Affairs to obtain detailed information from assets' owners and operators.
- The Minister for Home Affairs to direct an owner or operator "to do, or not to do, a specified thing to mitigate against a national security risk where all other mechanisms to mitigate the risk have been exhausted." [28]

The Security of Critical Infrastructure Act 2018 and subsequent expansive amendments reflect the Commonwealth's assertion that "the best way to protect Australians at scale is to secure [its] critical infrastructure." [29] Although the Australian government's overall cybersecurity

[†] The Government Communications Headquarters is the British signals intelligence agency; its U.S. equivalent is the National Security Agency.

strategy invariably characterizes its relationship with the private sector as a partnership, its tone toward the critical infrastructure sector is markedly different. Private ownership notwithstanding, Australia's regulatory framework for the critical infrastructure reflects the sector's indispensability to its citizens and national security. This should be instructive for the United States, where most critical infrastructure is privately owned and operated,[30] overseen by a patchwork of sector-specific regulatory agencies' authorities to impose fines and other penalties on specific companies for failing to adhere to sufficient cybersecurity practices.[31] NCSC and CIC are both useful organizational models by which the United States should reconsider CISA's role in public-private cybersecurity efforts, but in CIC one can see the reach of such a model when reinforced by a legislative mandate.

CISA

The Cybersecurity and Infrastructure Agency (CISA) is responsible for leading the national effort to manage cyber and physical risk to critical infrastructure.[32] In 2002, responsibility for designation and protection of critical infrastructure was given to the newly-established Department of Homeland Security's (DHS) Directorate of Information Analysis and Infrastructure Protection.[33] Resources allocated to DHS's critical infrastructure mission increased in relation to policymakers' understanding of the issue in the context of national security. What began as a relatively small component of DHS grew into the National Protection and Programs Division (NPPD) in 2007, and eventually into CISA in 2018, a federal agency under DHS, but on par with the U.S. Secret Service or FEMA.[34]

To keep pace with the inherent risks to the cybersecurity of critical infrastructure caused by rapidly evolving technologies and their associated threat vectors, Congress is working to strengthen CISA. In the House, the Safe Communities Act of 2020 and the Cybersecurity

Advisory Committee Authorization Act of 2019 would, respectively require CISA to maintain a clearinghouse of security guidance to enhance its outreach to critical infrastructure stakeholders - and - require DHS to establish an advisory committee within CISA to better how it executes its mission.[35] In the Senate, the Cybersecurity Vulnerability Identification and Notification Act of 2019 and the Small Business Advanced Cybersecurity Enhancements Act of 2018 would, respectively grant CISA subpoena power to receive information about security vulnerabilities - and - direct the Small Business Administration to create cybersecurity assistance units to interface with small businesses to exchange cyber threat indicators.[36] Despite bipartisan sponsorship and the promise of improving aspects of CISA, the four referenced bills lack any overarching regulatory or procedural framework for the public-private partnership.

The 2016 *National Cyber Security Strategy* (UK) rightly identifies securing its national cyberspace as a "collective effort" between government and the private sector, acknowledging that "although key sectors of [its] economy are in private hands, Government is ultimately responsible for assuring national resilience."[37] The United States should adopt the same approach, summarized by former Senator Barbara Mikulski as: ".gov" must help ".com."[38] The Commission recommends NCSC serve as a model for CISA's public sector outreach and is why proposed legislation currently in Congress places an emphasis on private sector engagement. But of the four referenced bills, only the Cybersecurity Vulnerability Identification and Notification Act of 2019 provides CISA with teeth, in the form of administrative subpoena power to compel private sector compliance with requests to produce information about "security vulnerabilities relating to critical infrastructure in the information systems and devices of public and private entities."[39] Mandating industry- and sector-specific standards of cybersecurity through statutory means is a contentious topic.

In 2012, the Senate considered the Cybersecurity Act of 2012 (CSA2012) to "enhance the security and resiliency of the cyber and communications infrastructure of the United States" by establishing a public-private National Cybersecurity Council (NCC) to establish sector-specific "requirements for securing critical infrastructure."[40] Two key factors led to the bill's failure, best described by Clarke and Knake as "privacy and the r word."[41] First, private-sector opposition on the grounds that mandating private sector standards would be "anti-business" amendments to the bill that instead called for "voluntary outcome-based cybersecurity practices."[42] There were justifiable privacy and civil liberties concerns at the prospect of the U.S. government having access to private sector information that could include citizens' personal communications, banking information, or healthcare records, but, private sector resistance to government regulation drove changes to the bill. The PCIP's calculated omission of mandated standards in 1997 seemingly gave adherents to Milton Freidman's theories on government regulation of business a fifteen-year head start in crafting an argument against mandated standards.[43]

Second, an opinion championed in the Senate by the late John S. McCain that DHS should cede responsibility for the NCC and related efforts to the Department of Defense (DOD), specifically to U.S. Cyber Command (USCYBERCOM) and the National Security Agency (NSA).[44] While USCYBERCOM and NSA easily outmatch DHS in a comparison of manpower and broad experience in cybersecurity, this position is weakened by two points. First, a core DHS task since its founding is defense against threats to U.S. critical physical and cyber infrastructure through CISA and its precursor, the NPPD.[45] Critical infrastructure is a niche field, especially when viewed through the lens of cybersecurity; DHS possesses the expertise required to lead such an effort. Second, USCYBERCOM and NSA are DOD entities responsible for national cyber defense and foreign cyber threat intelligence, respectively.[46] Beyond its advisory role to

DHS, a more active involvement by DOD in domestic critical infrastructure networks has the potential to raise similar civil liberties concerns.[47] In the end, the bill was defeated 51-47. Eight years later, the United States is only incrementally closer to standardized cybersecurity for critical infrastructure.

Strengthening CISA

Legislation must provide CISA with the size, resources, and statutory authority to provide U.S government guidance and assistance to private sector cybersecurity. CISA should be elevated within DHS from its' status as a "headquarters element" to an "operational agency" (similar to the NSA's relationship to the Department of Defense).[48] This increase in status must be accompanied by an in-kind increase in funding to expand CISA's workforce and facilities. CISA's relationship with NSA should mirror that of the NCSC's with GCHQ. However, this relationship must be codified in a way that assuages the concerns of civil rights and privacy advocates by clarifying the methods for handling private sector data that could potentially include personal information of U.S. citizens by establishing limited conditions for retention and detailed procedures for protecting citizens' privacy. This process must be subject to oversight by the Department of Justice. DOD and Intelligence Community roles must be clearly defined as advisory; there must be no ambiguity. Congress must ensure that private companies are equipped to assure and educate their customers, employees, and shareholders on the conditions under which the government is involved in their networks; CISA's mission is security of critical infrastructure, not to serve as an enabler for offensive cyber operations.[49] CISA must possess standing authority to continuously monitor threat activity across all ".gov" networks.[50] CISA must possess subpoena power to compel companies to produce cyber threat and incident information. Legislation must specify mandatory cybersecurity standards for all American

companies that own or operate elements of critical infrastructure. Because industry requirements differ, the National Institute of Standards and Technology (NIST) framework should serve as a baseline, as it can be tailored to each company's unique needs.[51] The U.S. Chamber of Commerce supports private sector adoption of the NIST framework when incentivized through legal liability protections; this practice should continue if the measures will aid companies in reaching mandatory compliance.[52] Finally, confusion surrounding regulatory responsibilities for the private sector are attributable, in part, to a lack of focused oversight; congressional committees with oversight of healthcare and financial services should not be the decision-points for the cybersecurity of hospitals and banks, respectively. The oversight role of Congress must be clear.

Oversight

The Solarium Commission recommends that Congress establish House Permanent Select and Senate Permanent Select Committees on Cybersecurity.[53] As of January 2020, the 116th Congress held at least thirteen hearings involving cybersecurity by seven different congressional committees - three in the House and four in the Senate; and, during the 115th Congress, fifty-six hearings involving cybersecurity by seventeen different congressional committees - eight in the House and seven in the Senate.[54] Membership for permanent oversight committees should begin with majority and minority leadership from the respective House and Senate Committees on Appropriations, Armed Services, Banking, Commerce, Foreign Relations, Homeland Security & Governmental Affairs, Intelligence, Judiciary, and members appointed from the House and Senate at large. The committees should have jurisdiction over all things cybersecurity and be referred all proposed legislation concerning cybersecurity, organization/reorganization of agencies relating to cybersecurity, and authorizations for appropriations concerning

cybersecurity. The Senate Committee on Rules and Administration has been considering a resolution proposing the establishment of a Senate Select Committee on Cybersecurity since early 2017.[55] Shifting cybersecurity to a dedicated committee in each chamber would allow for focused attention to the topic rather than its consideration through the lens of other committee business (e.g., cybersecurity in the context of banking).

Cyber Diplomacy

In 2002, the United Nations (UN) General Assembly requested the Secretary-General "to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them" through the establishment of "a group of governmental experts."[56] Since 2004, the UN Group of Governmental Experts (GGE) has convened seven times to consider the applicability of International Law to cyberspace. While these efforts have moved slowly, modest progress has been achieved. The GGE's 2013 report concluded that international law applies to cyberspace and is "essential to maintaining peace and stability."[57] The GGE's 2015 report included voluntary "norms of responsible State behaviour" and "confidence building measures" to "strengthen international peace and security."[58] Unfortunately, the 2016-2017 GGE reached an impasse over the applicability of international law to cyberspace. The State Department's remarks following the 2016-2017 GGE attributed the breakdown to a minority of the participants, noting that this GGE's arrival at "common understandings on the implementation of stabilizing measures, including voluntary, non-binding norms of responsible State behavior in cyberspace and confidence building measures" had been in vain.[59] Despite this setback, the Commission notes that the GGE remains a "productive venue" for the United States to engage with other states to establish "shared understandings of acceptable behavior in cyberspace."[60] Illustrating the importance of this issue, Microsoft's Paul

Nicholas noted that "the world lacks a common space for finding out the facts about cyberattacks, for learning from others, for interpreting laws and for agreeing who did what to whom."[61] These remarks followed a workshop at the 2018 Munich Security Conference discussing gaps in international law as it applies to cyberspace; part of a larger effort on behalf of the Microsoft Corporation to organize private sector support for initiatives with similar aims of the various GGEs; global inclusion with global governance.

On the United States' approach to understanding the digital world, Laura Rosenberger offers a critique similar to Schadlow's; the United States' "tactical" view of its information contest with Russia and China ignores the convergence of cyberspace and the information space.[62] Similar to counterterrorism as an aspect of foreign policy, the complexity of cybersecurity requires a "whole of government" approach. EO 13800 of May 11, 2017 directs the Secretaries of State, Treasury, Defense, Commerce and Homeland Security to report their departments' international cybersecurity priorities to the President, then subsequently coordinate through the Secretary of State to provide a final "engagement strategy for international cooperation in cybersecurity."[63] The State Department complied with EO 13800 by developing five objectives to achieve the United States' "vision for cyberspace," four of which involve international engagement: increase international stability and reduce the risk of conflict stemming from the use of cyberspace; uphold an open and interoperable Internet where human rights are protected and freely exercised and where cross-border data flows are preserved; maintain the essential role of non-governmental stakeholders in how cyberspace is governed; and, advance an international regulatory environment that supports innovation and respects the global nature of cyberspace.[64] Similarly, subsequent DOD and DHS cybersecurity strategies identified objectives specific to their respective responsibilities.[65]

Single Point of Success

In October 2001, President Bush created the position of Special Advisor to the President for Cyberspace Security ("cyber czar") to coordinate cybersecurity policy across the U.S. government and to chair the newly established President's Critical Infrastructure Protection Board.[66] During his tenure as the inaugural "cyber czar," Richard A. Clarke recalls efforts within the White House to limit the position's authority as he attempted to prioritize private sector engagement.[67] When Clarke left government in 2003, the Bush Administration left the position vacant. At President Obama's direction in 2009, the White House Office of Science and Technology Policy (OSTP) conducted a sixty-day review of U.S. cybersecurity policy. First among OSTP's ten proposed "near-term" actions was a recommendation to "appoint a cybersecurity policy official responsible for coordinating [U.S.] cybersecurity policies and activities," citing the absence of a "single individual or entity" with this responsibility.[68] OSTP asserted that "anchoring" this position at the White House would both signal the United States' seriousness about cybersecurity, and allow the position to leverage the Executive Office of the President (EOP) to "harmonize disparate responsibilities and authorities."[69] In December 2009, President Obama appointed Howard Schmidt as the first White House Cybersecurity Coordinator. Although Schmidt possessed ample qualifications from service in the private-sector and as a cybersecurity advisor in the Bush Administration, critics noted that the Cybersecurity Coordinator reported to the Deputy National Security Advisor instead of directly to the President.[70] In a similar criticism, Clarke notes that "few qualified people wanted the job" because its structure required reporting to the National Economic Advisor and the National Security Advisor, giving it "no apparent authority."[71]

The Clinton Administration and each of its successors recognized that public-private intersection in critical infrastructure necessitates coordination between an administration's economic and national security staffs. With oversight of critical infrastructure cybersecurity an eponymous aspect of its core function, such a reporting arrangement for the Cybersecurity Coordinator would appear logical. Two points suggest otherwise. First, to be certain, "czars" can exert significant influence on government policy and operations involving their specific focus areas, i.e. the "drug czar" leading the Office of National Drug Control Policy can affect DOD counternarcotics strategy or Drug Enforcement Administration priorities. However far-reaching the effects of this influence, it does not equate to the same legal authority exercised by those occupying Presidential Appointment with Senate Confirmation (PAS) positions. Louis Fisher characterizes the activities of non-PAS "czars" in the "shaping and execution of federal programs" as a constitutional concern because they parallel the actions of "officials confirmed to do precisely that."[72] Absent statutory authority, the Cybersecurity Coordinator's efficacy is defined by the officer-holder's standing within an administration, and by extension, with the President. Second, the debate over CSA2012 demonstrated that critical infrastructure security ceases to be viewed exclusively through a national security lens when considering private sector roles and responsibilities in the effort. Clarke illustrates this with a recounting of Obama Administration Economic Advisor Larry Sommers's dismissal of government regulation of the private sector to reduce critical infrastructure vulnerability on the basis that industry and "market forces would do enough" to address threats.[73]

Regardless of a Cybersecurity Coordinator's level of expertise, advice offered by individuals occupying this position lacks the force of statutory authority and is subject to interpretation by higher-ranking non-PAS officials in the NSC and National Economic Council.

Applying the latter interpretation to cybersecurity guidance risks either a dilution or distortion of objective expert input. An unrelated example of this was on display during May 12, 2020 and June 30, 2020 hearings before the Senate Committee on Health, Education, Labor, and Pensions in which Senator Rand Paul questioned National Institute of Allergy and Infectious Diseases Director Dr. Anthony Fauci's qualifications to make decisions concerning the reopening of schools and continuation of professional sports in the United States during the 2019 novel coronavirus disease (COVID-19) pandemic. In both hearings, Dr. Fauci informed the Senator that his guidance stemmed from a science-based focus on public health and meant to inform, rather than supplant, policy- and decisionmakers. As a career appointed official, Dr. Fauci's presence in this position is less an appointment than an ascension by a careerist in a specialized field.

Following the April 2018 departure of Cybersecurity Coordinator Rob Joyce, the Trump Administration eliminated the position on the basis that it was redundant.[74] This exposes another weakness of "czars" – recognition that their positions need to exist is subjective. Despite demonstrable evidence of a cyber-enabled foreign disinformation campaign during the 2016 U.S. presidential election, the Trump Administration decided that cyber threats were best addressed on an agency-by-agency basis instead of under the guidance of a central coordinating figure.

Notes

1. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report* (Rosslyn, VA: Cyberspace Solarium Commission, 2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

2. Michael D. Watkins, "How to Think Strategically," *Harvard Business Review*, April 20, 2007, https://hbr.org/2016/12/4-ways-to-improve-your-strategic-thinking-skills.

3. Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York, The Free Press, 1990), 72.

4. Cohen and Gooch, 73.

5. Cohen and Gooch, 63.

6. Cohen and Gooch, 88.

7. David Stevens, "The Australian Corvettes," in *Papers in Australian Maritime Affairs: Australian Maritime Issues 2010: SPC-A Annual 35*, ed. Rhett Mitchell (Canberra: Commonwealth of Australia, 2011), 128-134, https://www.navy.gov.au/sites/default/files/documents/PIAMA35.pdf.

8. David Stevens, *A Critical Vulnerability: The Impact of the Submarine Threat on Australia's Maritime Defence 1915–1954* (Canberra: Commonwealth of Australia, 2005), chap. 6, https://www.navy.gov.au/sites/default/files/documents/PIAMA15.pdf.

9. *Critical Infrastructures Protection Act of 2001, U.S. Code* 42 (2002), § 5195c.

10. U.S. Library of Congress, Congressional Research Service, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, by Brian E. Humphreys, R45809 (2019), 2.

11. Ibid.

12. "Oklahoma City Bombing," Federal Bureau of Investigation, 2020, https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing.

13. "Executive Order 13010 of July 15, 1996, Critical Infrastructure Protection," *Federal Register* 61, no. 138 (July 17, 1996): 37347-37350, https://www.federalregister.gov/documents/1996/07/17/96-18351/critical-infrastructure-protection; "Executive Order 13025 of November 13, 1996, Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection," *Federal Register* 61, no. 223 (November 18, 1996): 58623, https://www.govinfo.gov/content/pkg/FR-1996-11-18/pdf/96-29597.pdf.

14. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: President's Commission on Critical Infrastructure Protection, 1997), https://fas.org/sgp/library/pccip.pdf.

15. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, x.

16. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, 18.

17. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 106-107.

18. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, 27.

19. Ibid; Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 107-108.

20. Youngstown Sheet & Tube Co. v. Sawyer, 343 S. Ct. 579 (1952), https://supreme.justia.com/cases/federal/us/343/579/.

21. HM Government, *National Cyber Security Strategy* (London, United Kingdom: Exchequer, 2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

22. HM Government, *National Cyber Security Strategy*, 29.

23. Ibid; Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Los Angeles: CQ Press, 2017), 492.

24. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, 105-107.

25. Department of Home Affairs, *Critical Infrastructure Resilience Strategy: Plan* (Canberra: Commonwealth of Australia, 2015), https://cicentre.gov.au/document/P50S023.

26. Ibid, 2.

27. "What is the Critical Infrastructure Centre?" Department of Home Affairs, 2020, https://cicentre.gov.au/document/P50S010.

28. "The *Security of Critical Infrastructure Act 2018*," Department of Home Affairs, 2020, https://www.homeaffairs.gov.au/nat-security/files/cic-factsheet-security-of-critical-infrastructure-act-2018.pdf.

29. Department of Home Affairs, *Australia's Cyber Security Strategy 2020* (Canberra: Commonwealth of Australia, 2020), 28, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

30. "Critical Infrastructure Sector Partnerships," Cybersecurity and Infrastructure Security Agency, 2020, https://www.cisa.gov/critical-infrastructure-sector-partnerships.

31. Carrie Cordero and David Thaw, "The Cyberspace Solarium Commission's Mandate to Fix Congressional Oversight," *Lawfare* (blog), March 18, 2020, https://www.lawfareblog.com/cyberspace-solarium-commissions-mandate-fix-congressional-oversight.

32. "About CISA," Cybersecurity and Infrastructure Security Agency, 2020, https://www.cisa.gov/about-cisa.

33. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135(2002), https://www.congress.gov/bill/107th-congress/house-bill/5005; White House, *National Strategy to Secure Cyberspace* (Washington, DC: White House, 2003), 55, https://www.hsdl.org/?view&did=1040.

34. *Cybersecurity and Infrastructure Security Agency Act of 2018*, Public Law 115-278, U.S. Statutes at Large 132 (2018): 4169.

35. U.S. House of Representatives, *Safe Communities Act of 2020*, H. Res. 5780, 116th Cong., 2d sess., introduced in House February 6, 2020, https://www.congress.gov/116/bills/hr5780/BILLS-116hr5780rfs.pdf; U.S. House of Representatives, *Cybersecurity Advisory Committee Authorization Act of 2019*, H. Res. 1975, 116th Cong., 1st sess., introduced in House March 28, 2019, https://www.congress.gov/116/bills/hr1975/BILLS-116hr1975ih.pdf.

36. U.S. Senate, *Cybersecurity Vulnerability Identification and Notification Act of 2019*, S. 3045, 116th Cong., 1st sess., introduced in Senate December 12, 2019, https://www.congress.gov/116/bills/s3045/BILLS-116s3045rs.pdf; U.S. Senate, *Small Business Advanced Cybersecurity Enhancements Act of 2018*, S. 2735, 115th Cong., 2d Sess., introduced in Senate April 24, 2018, https://www.congress.gov/115/bills/s2735/BILLS-115s2735is.pdf.

37 HM Government, *National Cyber Security Strategy*, 27.

38. Senator Mikulski, speaking on S. 3414, on November 14, 2012, 112th Cong., 2nd sess., *Congressional Record* 158, pt. 11:15199.

39. *Cybersecurity Vulnerability Identification and Notification Act of 2019*.

40. U.S. Senate, *Cybersecurity Act of 2012*, S 2105, 112th Cong., 2d sess., introduced in Senate February 14, 2012, https://www.congress.gov/112/bills/s2105/BILLS-112s2105pcs.pdf.

41. Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 183.

42. R. Bruce Joston to Harry Reid and Mitch McConnell, January 30, 2012, in *U.S. Chamber of Commerce*, https://www.uschamber.com/sites/default/files/documents/files/120130_ComprehensiveCybersecurityLegislation_Reid_McConnell.pdf; U.S. Senate, *Cybersecurity Act of 2012*, S 3414, 112th Cong., 2d sess., introduced in Senate July 19, 2012, https://www.congress.gov/112/bills/s3414/BILLS-112s3414pcs.pdf.

43. Milton Friedman, "A Friedman Doctrine-- The Social Responsibility Of Business Is to Increase Its Profits," *New York Times Magazine*, September 13, 1970, https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html.

44. U.S. Senate, Committee on Homeland Security and Governmental Affairs, *Securing America's Future: The Cybersecurity Act of 2012: Testimony before the Committee on Homeland Security and Governmental Affairs*, 112th Cong., 2d sess., 2012.

45. White House, *National Strategy to Secure Cyberspace* (Washington, DC: White House, 2003), https://georgewbush-whitehouse.archives.gov/pcipb/cyberspace_strategy.pdf.

46. Keith B. Alexander to John McCain, May 4, 2012, cited in Ellen Nakashima, "NSA's Gen. Alexander: Companies should be required to fortify networks against cyberattack," *Washington Post*, May 4, 2012, https://www.washingtonpost.com/blogs/checkpoint-washington/post/nsas-gen-alexander-companies-should-be-required-to-fortify-networks-against-cyberattack/2012/05/04/gIQA1Snf1T_blog.html.

47. Ellen Nakashima, "Pentagon Proposes More Robust Role for its Cyber-Specialists," *Washington Post*, August 9, 2012, ProQuest.

48. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, 39.

49. Brad Smith, "Growing Consensus on the Need for an International Treaty on Nation State Attacks," *Microsoft* (blog), April 13, 2017, https://blogs.microsoft.com/on-the-issues/2017/04/13/growing-consensus-need-international-treaty-nation-state-attacks/.

50. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, 41.

51. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Washington, DC: Department of Commerce, 2019), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

52. "Preliminary Comments to the Cyberspace Solarium Commission," U.S. Chamber of Commerce, January 2020, https://www.uschamber.com/sites/default/files/short_paper_preliminary_u.s._chamber_comments_cyber_solarium_commission_final_last_revised_jan_31.pdf.

53. Cyberspace Solarium Commission, Cyberspace Solarium Commission Final Report, 39.

54. Carrie Cordero and David Thaw, *Rebooting Congressional Cybersecurity Oversight* (Washington, DC: CNAS, 2020), https://www.cnas.org/publications/reports/rebooting-congressional-cybersecurity-oversight.

55. U.S. Senate, *A Resolution Establishing the Select Committee on Cybersecurity*, S. Res. 23, 115th Cong., 1st sess., introduced in Senate January 24, 2017, https://www.congress.gov/115/bills/sres23/BILLS-115sres23is.pdf.

56. General Assembly resolution 56/19, *Developments in the field of information and telecommunications in the context of international security*, A/RES/56/19 (7 January 2002)

57. United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General*, A/68/98* (24 June 2013)

58. United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General*, A/70/174 (22 July 2015)

59. Michele Markoff, "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security" (remarks, 2016-2017 UN Group of Governmental Experts, New York, June 23, 2017), https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/.

60. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, 49-50.

61. Paul Nicholas, "Filling gaps in international law is essential to making cyberspace a safer place." *Microsoft* (blog), March 27, 2018, https://www.microsoft.com/en-us/cybersecurity/blog-hub/filling-the-gaps-in-international-law-is-essential-to-making-cyberspace-a-safer-place.

62. Nadia Schadlow, "Peace and War: The Space Between," *War on the Rocks* (blog), August 18, 2014, https://warontherocks.com/2014/08/peace-and-war-the-space-between/; Laura Rosenberger, "Making Cyberspace Safe for Democracy," *Foreign Affairs* 99, no. 3 (May-June 2020), https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.

63. "Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *Federal Register* 82, no. 93 (May 16, 2017): 22391-22397, https://www.govinfo.gov/content/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

64. Office of the Coordinator for Cyber Issues, "Recommendations to the President on Protecting American Cyber Interests through International Engagement," (official memorandum, Washington, DC: Department of State, 2018), https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Protecting-American-Cyber-Interests-Through-International-Engagement.pdf.

65. U.S. Department of Defense, *Summary: Department of Defense Cybersecurity Strategy 2018* (Washington, DC: Department of Defense, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; U.S. Department of Homeland Security, *Cybersecurity Strategy* (Washington, DC: Department of Homeland Security, 2018), https://www.hsdl.org/?view&did=810462.

66. "Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age," *Federal Register* 66, no. 202 (October 18, 2001): 53061-53071. https://www.govinfo.gov/content/pkg/FR-2001-10-18/pdf/01-26509.pdf.

67. Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 112.

68. Office of Science and Technology Policy, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: White House, 2009), https://www.hsdl.org/?view&did=740047.

69. Office of Science and Technology Policy, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 7.

70. Angie Drobnic Holan, "Coordinator Named, but does not Report Directly to the President," *Politifact* (blog), December 30, 2009, https://www.politifact.com/truth-o-meter/promises/obameter/promise/202/create-a-national-cyber-adviser-to-coordinate-secu/.

71. Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 118.

72. Louis Fisher, *Constitutional Conflicts Between Congress and the President*, 6th ed. (Lawrence, KS: University of Kansas Press, 2014), 39.

73. Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 118.

74. Nicole Perlroth and David E. Sanger, "White House Eliminates Cybersecurity Coordinator Role," *New York Times*, May 15, 2018, ProQuest.

Conclusion

One cannot ignore the role of politics in the United States' shortcomings in the areas examined by this paper. Policies are decided by officials who ultimately answer to a voting public wherein some constituencies carry more influence than others. The Department of Justice under the Obama Administration appears sensitive to an appearance that it was adopting a heavy hand toward domestic groups espousing platforms antithetical to its own. Paradoxically, the Administration of the first African American President of the United States appeared reluctant to address an element of society whose danger was driven in part by displeasure with the fact that the forty-fourth President of the United States was African American. Admittedly, *The Modern Militia Movement* was an imperfect messenger and deserved its depiction by PSI as an example of a "poor quality intelligence [report]."[1] However, consider Figures 2 and 3 alongside this comment by PSI about *The Modern Militia Movement*:

Figure 2. Trump supporters storm Capitol building in Washington, D.C. on January 6, 2021. Photo by Tayfun Coskun/Anadolu Agency via Getty Images

Figure 3. Trump Supporters Rally In Freedom Plaza in Washington, D.C. on January 5, 2021. Photo by Robert Nickelsberg via Getty Images.

> Most surprising to some, it identified as "the most common symbol displayed by militia members" the so-called "Gadsden Flag," featuring a coiled snake and the words, "Don't Tread on Me."… And while it may hold significance to members of the militia movement, it is considered by many to be a symbol of American patriotism, and a popular symbol at Tea Party rallies.[2]

It is unlikely the discredited author of *The Modern Militia Movement* feels vindication in the fact that Figure 2 depicts at least three Gadsen Flags outside of the U.S. Capitol during an insurrection or that Figure 3 depicts a Gadsen Flag beside at least one member of the Proud Boys, a group the Canadian government recently designated a terrorist organization. The link between unheeded warnings in 2009 and these images is neither direct nor simple.

Policymakers allowed the national security apparatus to apply a familiar approach to domestic counterterrorism. In and of itself, the approach was logical: establish trust within communities, solicit information, develop intelligence, then eliminate threats. The question becomes one of focus – on what or whom did this approach focus, and why? It is not unreasonable to assume that global terrorist threats have a domestic component by way of physical or psychological penetration (e.g., radicalization). Absent the context provided by classified intelligence reporting detailing homeland security threats and operating with the benefit of hindsight, this paper cannot fault an approach to domestic counterterrorism that includes awareness over communities vulnerable to radicalization. The latter should be a focus of efforts and a source of information, but not exclusively, and certainly not at the expense of demonstrable threats.

East Africa

The Trump Administration's singular *hard power* approach to foreign policy seemingly lacked both a *soft power* component and an understanding of how to balance the two into *smart power*. Its approach to counterterrorism in East Africa demonstrates strategic incoherence

whereby policymakers seemingly failed to comprehend the relationship between stability and opportunity. For regional states, these opportunities manifest themselves in development projects facilitated by willing investors seeking relationships and profits in a stable environment. For the United States, stability is a component of CVE strategy, thereby limiting the ability of localized threats to develop into regional or transnational threats to U.S. interests. Moreover, regional stability and local security allow for more demonstrations of U.S. soft power such as USAID. Concurrent counterterrorism or security operations conducted in proximity to strategic competitors present opportunities to leverage access and placement from which to illuminate competitors' malign activity through information operations. As part of an overarching strategy, each of these efforts could combine to enhance U.S. influence in the region.

Without an inclination to view a U.S. presence in one country of low strategic importance as an opportunity to frustrate strategically important competitors such as Russia and China, an Administration will view a reduction in U.S. presence as a cost-saving exercise. There is also the matter of patience. In *Doing What You Know: The United States and 250 Years of Irregular War*, David E. Johnson characterizes patience as "politically abnormal" due to a "pervasive American trait that demands continued, if not immediate, success for the support of non-existential conflicts."[3] Johnson's point extends beyond an Administration's point of view, into the realm of its willingness to publicly endorse counterterrorism operations as worth the risk and to educate the public on a rationale for the cost. With respect to foreign policy in East Africa, further study could ascertain the political influence of the Somali diaspora in the United States to discover whether or not foreign aid has a potent political constituency.

Cybersecurity

Cybersecurity is domestic and foreign policy involving dynamic, evolving threats by state and non-state actors against public and private interests. The United States' lack of a coherent cybersecurity policy – particularly decentralized Executive authority and Congressional oversight – creates a strategic vulnerability to cyberterrorism. As of this writing, the Biden Administration has announced the President's intent to nominate the inaugural National Cyber Director (NCD), a position created by Congress in the National Defense Authorization Act for Fiscal Year 2021. The NCD's operational relationship with other entities such as NSA and USCYBERCOM remains unclear, undefined, and untested. As these develop over time to form precedent and institutional norms, the NCD and Congress must address the issue of mandatory cybersecurity standards for privately owned and operated critical infrastructure. International organizations offer fora in which to address norms in cyberspace; a favorable outcome is not a foregone conclusion, but the United States' domestic treatment of the problem will bolster its position in a multilateral effort. This is no different than diplomatic initiatives involving climate change or human rights. Standing, full committees in the U.S. Senate and House of Representatives dedicated to cybersecurity will foster informed oversight and legislation on cyber issues. *These* are the proper forums in which to debate the merits of regulatory policies, where experts focus on processes to further protection and resilience.

Notes

1. U.S. Senate, Committee on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report: Permanent Subcommittee on Investigations*, 105.

2. Ibid.

3. David E. Johnson, *Doing What You Know: The United States and 250 Years of Irregular War* (Washington, DC: Center for Strategic and Budgetary Assessments, 2017), 75, https://csbaonline.org/uploads/documents/CSBA6285_(COIN_Report)_Web.pdf.

Bibliography

Abu-Ras, Wahiba and Soleman Abu-Bader. "The Impact of the September 11, 2001, Attacks on the Well-being of Arab Americans in New York City." *Journal of Muslim Mental Health 3*, no. 2 (2008): 217-239. https://doi.org/10.1080/15564900802487634.

Arab American Institute Foundation. *Profiling and Pride: Arab American Attitudes and Behavior Since September 11*. Washington, DC: Arab American Institute Foundation, 2003. ProQuest.

Baker, Wayne, Ronald Stockton, Sally Howell, Amaney Jamal, Ann Chih Lin, Andrew Shryock, and Mark Tessler. *Detroit Arab American Study (DAAS) ICPSR04413-v2*. Ann Arbor, MI: Interuniversity Consortium for Political and Social Research [distributor], 2006. https://doi.org/10.3886/ICPSR04413.v2.

Bartlett, Jamie, and Carl Miller. "The Edge of Violence: Towards Telling the Difference Between Violent and Non-Violent Radicalization." *Terrorism and Political Violence 24*, no. 1 (2012): 1–21. https://doi.org/10.1080/09546553.2011.594923.

Bergen, Peter and Jennifer Rowland. "Right-wing Extremist Terrorism as Deadly a Threat as al Qaeda?" CNN, August 8, 2012. https://edition.cnn.com/2012/08/07/opinion/bergen-terrorism-wisconsin/index.html.

bin Laden, Usama. Usama bin Laden to Mukhtar Abu al-Zubayr, August 7, 2010. In Combating Terrorism Center at West Point. https://ctc.usma.edu/wp-content/uploads/2013/10/Letter-from-Usama-Bin-Laden-to-Mukhtar-Abu-al-Zubayr-Trnaslation.pdf.

Bolton, John R. "Remarks by National Security Advisor Ambassador John R. Bolton on the Trump Administration's New Africa Strategy." Washington, DC, December 12, 2018. https://www.whitehouse.gov/briefings-statements/remarks-national-security-advisor-ambassador-john-r-bolton-trump-administrations-new-africa-strategy/.

Bremmer, Ian. "The Winners of Trump's Foreign Policy: Year One." *Horizons: Journal of International Relations and Sustainable Development*, no. 10 (2018): 96-103. https://doi.org/10.2307/48573480.

Bruton, Bronwyn E. and Williams, Paul D. *Counterinsurgency in Somalia: Lessons Learned from the African Union Mission in Somalia, 2007-2013*. JSOU Report 14-5. Tampa, FL: Joint Special Operations University, 2014. https://www.socom.mil/JSOU/JSOUPublications/JSOU14-5_BrutonWilliams_AMISOM_FINAL.pdf.

Burke, Jason. "Trump's Offensive to 'Wipe Out' al-Shabaab Threatens More Pain for Somalis." *The Guardian*, April 22, 2017. https://www.theguardian.com/world/2017/apr/22/us-action-al-shabaab-somalia-millions-famine-drought.

Center for Strategic and International Studies Commission on Smart Power. *CSIS Commission on Smart Power: A Smarter, More Secure America*. Washington, DC: Center for Strategic and International Studies, 2007. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/071106_csissmartpowerreport.pdf.

Central Intelligence Agency. "Somalia," 2020. https://www.cia.gov/library/publications/the-world-factbook/geos/so.html.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, HarperCollins, 2010.

Cloud, David S. "U.S. Military Secretly Sent Small Team of Advisors to Somalia." *Los Angeles Times*, January 10, 2014. ProQuest.

Cohen, Eliot A. and John Gooch. *Military Misfortunes: The Anatomy of Failure in War*. New York: The Free Press, 1990.

Confucius. "Book XII, YEN YUAN." In *The Analects of Confucius (from the Chinese Classics)*, translated by James Legge, Chap. I. 1. Project Gutenberg, n.d. https://www.gutenberg.org/cache/epub/3330/pg3330.html.

Cordero, Carrie and David Thaw. "The Cyberspace Solarium Commission's Mandate to Fix Congressional Oversight." *Lawfare* (blog), March 18, 2020. https://www.lawfareblog.com/cyberspace-solarium-commissions-mandate-fix-congressional-oversight.

Cordero, Carrie and David Thaw. *Rebooting Congressional Cybersecurity Oversight*. Washington, DC: Center for a New American Security, 2020. https://www.cnas.org/publications/reports/rebooting-congressional-cybersecurity-oversight.

Cornwell, Paige. "FBI's Bus Ads Taken Down Over Muslim/Terrorist Stereotyping." *Seattle Times*, June 26, 2013. https://www.seattletimes.com/seattle-news/fbirsquos-bus-ads-taken-down-over-muslim-terrorist-stereotyping/.

Coutou, Diane. "Smart Power." *Harvard Business Review*, November 2008. https://hbr.org/2008/11/smart-power/.

Critical Infrastructures Protection Act of 2001, U.S. Code 42 (2002), § 5195c.

Cybersecurity and Infrastructure Security Agency. "About CISA," 2020. https://www.cisa.gov/about-cisa.

Cybersecurity and Infrastructure Security Agency Act of 2018, Public Law 115-278, *U.S. Statutes at Large* 132 (2018): 4169.

Cybersecurity and Infrastructure Security Agency. “Critical Infrastructure Sector Partnerships,” 2020. https://www.cisa.gov/critical-infrastructure-sector-partnerships.

Cyberspace Solarium Commission. *Cyberspace Solarium Commission Final Report*. Rosslyn, VA: Cyberspace Solarium Commission, 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

Davis, Jeff. "Statement by Pentagon Spokesman Capt. Jeff Davis on U.S. Counterterrorism Operations in Somalia." Department of Defense press release, March 30, 2017. On the Department of Defense website. https://www.defense.gov/Newsroom/Releases/Release/Article/1135338/statement-by-pentagon-spokesman-capt-jeff-davis-on-us-counterterrorism-operatio/.

Davis, Julie Hirschfled, Sheryl Gay Stolberg, and Thomas Kaplan. "Trump Alarms Lawmakers with Disparaging Words for Haiti and Africa." *New York Times*, January 11, 2018. ProQuest.

Dawsey, Josh. "Trump Derides Protections for Immigrants from 'Shithole' Countries." *Washington Post*, January 12, 2018. ProQuest.

de Tocqueville, Alexis. 1956. On Democracy, edited by Richard D. Heffner. New York: New American Library of World Literature.

Department of Home Affairs. *Australia’s Cyber Security Strategy 2020*. Canberra: Commonwealth of Australia, 2020. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Department of Home Affairs. *Critical Infrastructure Resilience Strategy: Plan*. Canberra: Commonwealth of Australia, 2015. https://cicentre.gov.au/document/P50S023.

Department of Home Affairs. "The Security of Critical Infrastructure Act 2018," 2020. https://www.homeaffairs.gov.au/nat-security/files/cic-factsheet-security-of-critical-infrastructure-act-2018.pdf.

Department of Home Affairs. "What is the Critical Infrastructure Centre?" 2020. https://cicentre.gov.au/document/P50S010.

Ellis, Heidi B. and Saida Abdi. 2017. “Building Community Resilience to Violent Extremism through Genuine Partnerships.” *American Psychologist* 72, no. 3 (April 2017): 289–300. https://doi:10.1037/amp0000065.

"Executive Order 13010 of July 15, 1996, Critical Infrastructure Protection." *Federal Register* 61, no. 138 (July 17, 1996): 37347-37350. https://www.federalregister.gov/documents/1996/07/17/96-18351/critical-infrastructure-protection.

"Executive Order 13025 of November 13, 1996, Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection." *Federal Register* 61, no. 223 (November 18, 1996): 58623. https://www.govinfo.gov/content/pkg/FR-1996-11-18/pdf/96-29597.pdf.

"Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age." *Federal Register* 66, no. 202 (October 18, 2001): 53061-53071. https://www.govinfo.gov/content/pkg/FR-2001-10-18/pdf/01-26509.pdf.

"Executive Order 13536 of April 12, 2010, Blocking Certain Persons Contributing to the Conflict in Somalia." *Federal Register* 75, no. 72 (April 15, 2010): 19869-19872. https://www.govinfo.gov/content/pkg/FR-2010-04-15/pdf/2010-8878.pdf.

"Executive Order 13584 of September 9, 2011, Developing an Integrated Strategic Counterterrorism Communications Initiative and Establishing a Temporary Organization to Support Certain Government-wide Communications Activities Directed Abroad." *Federal Register* 76, no. 179 (September 15, 2011): 56945-56947. https://www.govinfo.gov/content/pkg/FR-2011-09-15/pdf/2011-23891.pdf.

"Executive Order 13620 of July 20, 2012, Taking Additional Steps to Address the National Emergency With Respect to Somalia." *Federal Register* 77, no. 142 (July 24, 2010): 43483-43485. https://www.govinfo.gov/content/pkg/FR-2012-07-24/pdf/2012-18237.pdf.

"Executive Order 13675 of August 5, 2014, Establishing the President's Advisory Council on Doing Business in Africa." *Federal Register* 79, no. 153 (August 8, 2014): 46661-46663. https://www.govinfo.gov/content/pkg/FR-2014-08-08/pdf/2014-18998.pdf.

"Executive Order 13721 of March 14, 2016, Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584." *Federal Register* 81, no. 52 (March 17, 2016): 14685-14688. https://www.govinfo.gov/content/pkg/FR-2016-03-17/pdf/2016-06250.pdf.

"Executive Order 13746 of November 3, 2016 Advancing the Goals of the Power Africa Initiative to Expand Access to Electricity in Sub-Saharan Africa Through the Establishment of the President's Power Africa Working Group." *Federal Register* 81, no. 216 (November 8, 2016): 78697-78700. https://www.govinfo.gov/content/pkg/FR-2016-11-08/pdf/2016-27156.pdf.

"Executive Order 13769 of January 27, 2017, Protecting the Nation From Foreign Terrorist Entry Into the United States." *Federal Register* 82, no. 20 (February 1, 2017): 8977-8982. https://www.govinfo.gov/content/pkg/FR-2017-02-01/pdf/2017-02281.pdf.

"Executive Order 13780 of March 6, 2017, Protecting the Nation From Foreign Terrorist Entry Into the United States." *Federal Register* 82, no. 45 (March 9, 2017): 13209-13219. https://www.govinfo.gov/content/pkg/FR-2017-03-09/pdf/2017-04837.pdf.

"Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." *Federal Register* 82, no. 93 (May 16, 2017): 22391-22397. https://www.govinfo.gov/content/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

Federal Bureau of Investigation. "Crime in the United States - 2001." Uniform Crime Reporting Program, 2002. https://ucr.fbi.gov/crime-in-the-u.s/2001.

Federal Bureau of Investigation. "Oklahoma City Bombing," 2020. https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing.

Federal Bureau of Investigation. *White Supremacist Recruitment of Military Personnel since 9/11*. Washington, DC: Federal Bureau of Investigation, 2008. https://documents.law.yale.edu/sites/default/files/White%20Supremacist%20Recruitment%20of%20Military%20Personnel%20Since%209-11-ocr.pdf.

Felter, Clarie and Masters, Jonathan and Sergie, Mohammed Aly. "Al-Shabab." Council on Foreign Relations. Last modified January 10, 2020. https://www.cfr.org/backgrounder/al-shabab.

Finney, Nathan. "A Culture of Inclusion: Defense, Diplomacy, and Development as a Modern American Foreign Policy." *Small Wars Journal* (blog), September 26, 2010. https://smallwarsjournal.com/blog/journal/docs-temp/553-finney.pdf.

Fisher, Lewis. *Constitutional Conflicts Between Congress and the President*. Lawrence, KS: University of Kansas Press, 2014.

Flynn, Meagan. "'Malignant, Dangerous, Violent': Trump Rally's 'Send her Back!' Chant Raises New Concerns of Intolerance." *Washington Post*, July 18, 2019. ProQuest.

Freskos, Brian. "Anti-Terror Agency Points to N.C. Case as Example of Success." *Star-News*, Feb 22, 2013. ProQuest.

Friedman, Milton. "A Friedman Doctrine - The Social Responsibility of Business is to Increase Its Profits." *New York Times Magazine*, September 13, 1970. https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html.

Garthoff, Raymond. *Détente and Confrontation: American-Soviet Relations from Nixon to Reagan*, rev. ed. Washington, DC: Brookings, 1994.

Goldberg, Jeffrey. "The Obama Doctrine." *The Atlantic*, April 2016. https://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/.

Goldman, Adam and Matt Apuzzo. "Inside the Spy Unit That NYPD Says Doesn't Exist." *Associated Press*, August 31, 2011. ProQuest.

Greer, Ryan, Tony Blair, Daniel F. Runde, Enrique Betancourt, Paul M. Bisca, Todd Diamond, Emman El-Badawy, Ryan Greer, Olivier Lavinal, and Rebecca Wolfe. *Sharpening Our Efforts: The Role of International Development in Countering Violent Extremism*. Report. Edited by Yayboke Erol K. and Ramanujam Sundar R. Washington, DC: Center for Strategic and International Studies, 2019. https://doi.org/10.2307/resrep22565.9.

HM Government. *National Cyber Security Strategy*. London: Exchequer, 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Holan, Angie Drobnic. "Coordinator Named, but does not Report Directly to the President." *Politifact* (blog), December 30, 2009. https://www.politifact.com/truth-o-meter/promises/obameter/promise/202/create-a-national-cyber-adviser-to-coordinate-secu/.

Homeland Security Advisory Council. *Countering Violent Extremism (CVE) Working Group*. Washington, DC: Department of Homeland Security, 2010. https://permanent.fdlp.gov/gpo20410/hsac-cve-working-group-recommendations.pdf.

Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, *U.S. Statutes at Large* 118 (2004): 3644.

International Committee of the Red Cross. "How is the Term "Armed Conflict" Defined in International Humanitarian Law?" 2008. https://www.icrc.org/en/doc/assets/files/other/opinion-paper-armed-conflict.pdf.

Johnson, Daryl. "I Warned of Right-wing Violence in 2009. Republicans Objected. I was Right." *Washington Post*, August 21, 2017. ProQuest.

Johnson, David E. *Doing What You Know: The United States and 250 Years of Irregular War*. Washington, DC: Center for Strategic and Budgetary Assessments, 2017. https://csbaonline.org/uploads/documents/CSBA6285_(COIN_Report)_Web.pdf.

Joint Chiefs of Staff. *Antiterrorism*. JP 3-07.2. Washington, DC: Joint Chiefs of Staff, 2010. https://www.hsdl.org/?view&did=753152.

Joston, R. Bruce. Bruce R. Joston to Harry Reid and Mitch McConnell, January 30, 2012. In U.S. Chamber of Commerce. https://www.uschamber.com/sites/default/files/documents/files/120130_ComprehensiveCybersecurityLegislation_Reid_McConnell.pdf.

Lake, Eli and Audrey Hudson. "Napolitano Stands by Controversial Report." *Washington Times*, April 16, 2009. ProQuest.

Liebkind, Karmela and Inga Jasinskaja-Lahti. The Influence of Experiences of Discrimination on Psychological Stress: A Comparison of Seven Immigrant Groups. *Journal of Community & Applied Social Psychology 10*, no. 1 (2000): 1–16. https://doi.org/10.1002/(SICI)1099-1298(200001/02)10:1<1::AID-CASP521>3.0.CO;2-5.

Lindsay, James M. Congress and the Politics of U.S. Foreign Policy. Baltimore: The Johns Hopkins University Press, 1994.

Longaker, Richard P. "The President as International Leader." *Law and Contemporary Problems* 21, no. 4 (1956): 735-752. https://doi.org/10.2307/1190193.

Los Angeles Times. "Overdone Outrage." April 17, 2009. ProQuest.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*, 7th ed. Los Angeles: CQ Press, 2017.

Luiijf, Eric. "Definitions of Cyber Terrorism." In *Cyber Crime and Cyber Terrorism Investigator's Handbook*, edited by Babak Akhgar, Andrew Staniforth and Francesca Bosco, 11-17. Oxford: Syngress, 2014. https://doi.org/10.1016/B978-0-12-800743-3.00002-5.

Markoff, Michele. "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security." United Nations, June 23, 2017. https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/.

McCrummen, Stephanie and Karen DeYoung. "U.S. Airstrike Kills Somali Accused of Links to Al-Qaeda." *Washington Post*, May 2, 2008. ProQuest.

McDermott, James. James McDermott to Robert Mueller, June 19, 2013. On the Representative James McDermott website. http://mcdermott.house.gov/images/pdf/facesterrorism.pdf

Miller, Joshua Rhett. "'Fusion Centers' Expand Criteria to Identify Militia Members." Fox News. Last modified December 24, 2015. https://www.foxnews.com/politics/fusion-centers-expand-criteria-to-identify-militia-members.

Missouri Information Analysis Center. *The Modern Militia Movement*. Jefferson City, MO: Missouri State Highway Patrol, 2009. https://thelastdemocrat.files.wordpress.com/2010/02/13290698-the-modern-militia-movementmissouri-miac-strategic-report-20feb09.pdf.

Naff, Alixa. "The Early Arab Immigrant Experience." In *The Development of Arab-American Identity*, edited by Ernest N. McCarus, 23-36. Ann Arbor: University of Michigan Press, 1994.

Nakashima, Ellen. "NSA's Gen. Alexander: Companies Should be Required to Fortify Networks Against Cyberattack," *Washington Post*, May 4, 2012. ProQuest.

Nakashima, Ellen. "Pentagon Proposes More Robust Role for its Cyber-Specialists," *Washington Post*, August 9, 2012. ProQuest.

Nakashima, Ellen, Shane Harris, Josh Dawsey, and Anne Gearan. "Senior Intelligence Official Told Lawmakers that Russia Wants to See Trump Reelected." *Washington Post*, February 21, 2020. ProQuest.

Nastios, Andrew S. "Foreign Aid in an Era of Great Power Competition." *PRISM* 8, no. 4 (2020). 101-119.

National Commission on Terrorist Attacks Upon the United States. *The 9-11 Commission Report*. Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004. https://govinfo.library.unt.edu/911/report/911Report.pdf.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Washington, DC: Department of Commerce, 2019. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

New America. "The War in Somalia," July 21, 2020. https://www.newamerica.org/international-security/reports/americas-counterterrorism-wars/the-war-in-somalia/.

New York City Police Department. *Egyptian Locations of Interest Report*. New York: New York City Police Department, 2006. https://hosted.ap.org/specials/interactives/documents/nypd/nypd-egypt.pdf.

Nicholas, Paul. "Filling Gaps in International Law is Essential to Making Cyberspace a Safer Place." *Microsoft* (blog), March 27, 2018. https://www.microsoft.com/en-us/cybersecurity/blog-hub/filling-the-gaps-in-international-law-is-essential-to-making-cyberspace-a-safer-place.

Nichols, Tom. The Death of Expertise. New York: Oxford University Press, 2017.

Nye, Joseph S. "Get Smart: Combining Hard and Soft Power." *Foreign Affairs* 88, no. 4. (2009): 160-63. JSTOR.

Nye, Joseph S. "Public Diplomacy and Soft Power." *The Annals of the American Academy of Political and Social Science* 616 (2008): 94-109. JSTOR.

Obama, Barack. "Remarks by the President at the Summit on Countering Violent Extremism." The White House, February 19, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/02/19/remarks-president-summit-countering-violent-extremism-february-19-2015.

Obama, Barack. "Remarks by the President at the United States Military Academy Commencement Ceremony." West Point, New York, May 28, 2014. https://obamawhitehouse.archives.gov/the-press-office/2014/05/28/remarks-president-united-states-military-academy-commencement-ceremony.

Obama, Barack. "Renewing American Leadership." *Foreign Affairs*, July-August 2007. https://www.foreignaffairs.com/articles/2007-07-01/renewing-american-leadership.

O'Connell, Vanessa, Stephanie Simon, and Evan Perez. "For the Love of Islam - A Second American Woman is Arrested in Cartoonist Case." *Wall Street Journal*, March 13, 2010, Eastern edition. ProQuest.

Office of the Director of National Intelligence. *Analytic Standards*. IC Directive 203. Washington, DC: Office of the Director of National Intelligence, 2015. https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

Office of the Director of National Intelligence. *Assessing Russian Activities and Intentions in Recent US Elections*. Washington, DC: National Intelligence Council, 2016. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Office of the Director of National Intelligence. *Sourcing Requirements for Disseminated Analytic Products*. IC Directive 206. Washington, DC: Office of the Director of National Intelligence, 2015. https://www.dni.gov/files/documents/ICD/ICD%20206.pdf.

Office of the Director of National Intelligence. *Tearline Production and Dissemination*. IC Directive 209. Washington, DC: Office of the Director of National Intelligence, 2012. https://www.odni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf.

Office of Science and Technology Policy. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: White House, 2009. https://www.hsdl.org/?view&did=740047.

O'Keefe, Ed. "Napolitano Defends Report on Extremism." *Washington Post*, April 16, 2009. ProQuest.

O'Keefe, Ed. "Napolitano Comments on 'Right Wing Extremist' Report." *Washington Post*, April 15, 2009. http://voices.washingtonpost.com/federal-eye/2009/04/napolitano_comments_on_right_w.html.

Pandith, Farah. "National Security Readiness Requires Cultural Listening." *Global Challenges* (blog), Tony Blair Institute for Global Change. January 10, 2019. https://institute.global/policy/national-security-readiness-requires-cultural-listening.

Paul, Kshemendra N. “Federal Resource Allocation Criteria.” Official memorandum. Washington, DC: Office of the Director of National Intelligence, 2011. https://www.dni.gov/files/ISE/documents/DocumentLibrary/RAC_final.pdf.

Parlapiano, Alicia. "The Flow of Money and Equipment to Local Police." *New York Times*, August 23, 2014, ProQuest.

Perlroth, Nicole and David E. Sanger. "White House Eliminates Cybersecurity Coordinator Role." *New York Times*, May 15, 2018. ProQuest.

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. Washington, DC, President's Commission on Critical Infrastructure Protection, 1997. https://fas.org/sgp/library/pccip.pdf.

President's Advisory Council on Doing Business in Africa. *Fact-Finding Trip Report and Recommendations*. Washington, DC: Department of Commerce, 2018. https://legacy.trade.gov/pac-dbia/docs/PAC-DBIA%20Final%20Report%20Sep%202018.pdf.

Rehbein, David K. David K. Rehbein to Janet Napolitano, April 13, 2009. In Fox News. https://www.foxnews.com/opinion/an-open-letter-to-homeland-security-on-rightwing-extremists.

Rose, Gideon. "What Obama Gets Right." *Foreign Affairs*, June 18, 2020. https://www.foreignaffairs.com/articles/2017-07-05/what-obama-gets-right.

Rosenberg, Eli and Paul Schemm, "‘Here is What my #shithole Looks Like’: African Countries and Haiti React to Trump’s Remark." *Washington Post*, January 12, 2018. ProQuest.

Rosenberger, Laura. "Making Cyberspace Safe for Democracy." *Foreign Affairs* 99, no. 3 (May-June 2020). https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.

Sanders, Sarah. "Press Briefing by Press Secretary Sarah Sanders and Dr Ronny Jackson." The White House, January 16, 2018. https://www.whitehouse.gov/briefings-statements/press-briefing-by-press-secretary-sarah-sanders-and-dr-ronny-jackson-01162018/.

Sanders, Sarah. "Press Briefing by Press Secretary Sarah Sanders." The White House, January 23, 2018. https://www.whitehouse.gov/briefings-statements/press-briefing-press-secretary-sarah-sanders-012318/.

Savage, Charlie and Schmidt, Eric. "Trump Eases Combat Rules in Somalia Intended to Protect Civilians." *New York Times*, March 30, 2017. ProQuest.

Schadlow, Nadia. "Peace and War: The Space Between." *War on the Rocks*, August 18, 2014. https://warontherocks.com/2014/08/peace-and-war-the-space-between/.

Seligman, Lester G. "The Presidential Office and the President as Party Leader." *Law and Contemporary Problems* 21, no. 4 (1956): 724-34. https://doi.org/10.2307/1190192.

Shultz, Richard. *Military Innovation in War: It Takes a Learning Organization*. JSOU Report 16-6. Tampa, FL: Joint Special Operations Univeristy, 2016. https://www.sofx.com/wp-content/uploads/2016/07/JSOU16-6_Shultz_TF714_final1.pdf.

Smith, Brad. "Growing Consensus on the Need for an International Treaty on Nation State Attacks," *Microsoft* (blog), April 13, 2017. https://blogs.microsoft.com/on-the-issues/2017/04/13/growing-consensus-need-international-treaty-nation-state-attacks/.

Smith, R. Jeffrey. "Homeland Security Department Curtails Home-grown Terror Analysis." *Washington Post*, June 7, 2011. ProQuest.

Stanford University. "Al Shabaab." January 2019. https://cisac.fsi.stanford.edu/mappingmilitants/profiles/al-shabaab.

Stares, Paul B. *Preparing for the Next Foreign Policy Crisis*. New York: Council on Foreign Relations, 2019. https://cdn.cfr.org/sites/default/files/report_pdf/Preparing%20for%20the%20Next%20Foreign%20Policy%20Crisis.pdf.

Stevens, David. *A Critical Vulnerability: The Impact of the Submarine Threat on Australia's Maritime Defence 1915–1954*. Canberra: Commonwealth of Australia, 2005. https://www.navy.gov.au/sites/default/files/documents/PIAMA15.pdf.

Stevens, David. "The Australian Corvettes." In *Papers in Australian Maritime Affairs: Australian Maritime Issues 2010: SPC-A Annual 35*, edited by Rhett Mitchell, 128-134. Canberra: Commonwealth of Australia, 2011. https://www.navy.gov.au/sites/default/files/documents/PIAMA35.pdf.

Trump, Donald J. "President Trump Campaign Rally in Minneapolis." Minneapolis, Minnesota, October 10, 2019. https://www.c-span.org/video/?464823-1/president-trump-holds-rally-minneapolis-minnesota&start=5599.

Trump, Donald J. "Remarks by President Trump in Cabinet Meeting." The White House, February 12, 2019. https://www.whitehouse.gov/briefings-statements/remarks-president-trump-cabinet-meeting-13/.

Trump, Donald J. "Remarks by President Trump at the 3rd Annual Made in America Product Showcase." The White House, July 19, 2019. https://www.whitehouse.gov/briefings-statements/remarks-president-trump-3rd-annual-made-america-product-showcase/.

Trump, Donald J. "Remarks by President Trump Before Marine One Departure." The White House, July 19, 2019. https://www.whitehouse.gov/briefings-statements/remarks-president-trump-marine-one-departure-53/.

Trump, Donald J. "Remarks by President Trump and President Iohannis of Romania Before Bilateral Meeting." The White House, August 20, 2019. https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-iohannis-romania-bilateral-meeting/.

Trump, Donald J. "Remarks by President Trump Before Marine One Departure." The White House, August 21, 2019. https://www.whitehouse.gov/briefings-statements/remarks-president-trump-marine-one-departure-60/.

United Nations. General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*. A/68/98* (24 June 2013).

United Nations. General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*. A/70/174 (22 July 2015).

United Nations. General Assembly. Resolution 56/19. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/56/19 (7 January 2002).

U.S. Agency for International Development. "Countering Violent Extremism in Kenya, Somalia, and East Africa," 2019. https://www.usaid.gov/sites/default/files/documents/1860/Countering_Violent_Extremism_fact_sheet_February_2019.pdf.

U.S. Agency for International Development. "Power Africa," 2020. https://www.usaid.gov/sites/default/files/documents/1860/PowerAfrica_Fact_Sheet06262020.pdf.

U.S. Agency for International Development. *The Development Response to Violent Extremism and Insurgency*. Washington, DC: U.S. Agency for International Development, 2019. https://www.usaid.gov/sites/default/files/documents/1870/VEI_Policy_Final.pdf.

U.S. Agency for International Development. "Transition Initiatives for Stabilization + (TIS+)," 2020. https://www.usaid.gov/sites/default/files/documents/1860/Fact-Sheet-Somalia-TISfeb-2020.pdf.

U.S. Chamber of Commerce. “Preliminary Comments to the Cyberspace Solarium Commission," January 2020. https://www.uschamber.com/sites/default/files/short_paper_preliminary_u.s._chamber_comments_cyber_solarium_commission_final_last_revised_jan_31.pdf.

U.S. Congress. *Congressional Record*. 112th Cong., 2nd sess., 2012. Vol. 158, pt. 11.

U.S. Department of Commerce. "Prosper Africa Toolkit: U.S. Government Trade and Investment Services," 2020. https://www.usaid.gov/sites/default/files/documents/1860/PowerAfrica_Fact_Sheet06262020.pdf.

U.S. Department of Defense. *Summary: Department of Defense Cybersecurity Strategy 2018*. Washington, DC: Department of Defense, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

U.S. Department of Homeland Security. *Cybersecurity Strategy*. Washington, DC: Department of Homeland Security, 2018. https://www.hsdl.org/?view&did=810462.

U.S. Department of Homeland Security. *Department of Homeland Security Information Sharing Strategy*. Washington, DC: Department of Homeland Security, 2008. https://www.hsdl.org/?view&did=486486.

U.S. Department of Homeland Security. *Domestic Extremism Lexicon*. Washington, DC: Department of Homeland Security, 2009. https://fas.org/irp/eprint/lexicon.pdf.

U.S. Department of Homeland Security. "National Network of Fusion Centers," 2014. https://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout_0.pdf.

U.S. Department of Homeland Security. *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment*. Washington, DC: Department of Homeland Security, 2009. https://fas.org/irp/eprint/rightwing.pdf.

U.S. Department of Homeland Security. "State and Major Urban Area Fusion Centers." 2012. https://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout_0.pdf.

U.S. Department of State. “Center for Strategic Counterterrorism Communications," 2011. https://2009-2017.state.gov/documents/organization/116709.pdf.

U.S. Department of State. "Foreign Terrorist Organizations," 2020. https://www.state.gov/foreign-terrorist-organizations/.

U.S. Department of State. Office of the Coordinator for Cyber Issues. “Recommendations to the President on Protecting American Cyber Interests through International Engagement.” Official memorandum. Washington, DC: Department of State, 2018. https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Protecting-American-Cyber-Interests-Through-International-Engagement.pdf.

U.S. Department of State. “U.S. Relations With Somalia: Bilateral Relations Fact Sheet," 2019. https://www.state.gov/u-s-relations-with-somalia/.

U.S. Government Accountability Office. *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*. GAO-17-300. Washington, D.C., 2017.

U.S. House of Representatives. Committee on Armed Services. *National Defense Authorization Act for Fiscal Year 2017: Report (to Accompany H.R. 4909)*. 114th Cong., 2d. sess., 2016. H. Rept. 114-537.

U.S. House of Representatives. *Cybersecurity Advisory Committee Authorization Act of 2019*. H. Res. 1975. 116th Cong., 1st sess. Introduced in House March 28, 2019. https://www.congress.gov/116/bills/hr1975/BILLS-116hr1975ih.pdf.

U.S. House of Representatives. *Safe Communities Act of 2020*. H. Res. 5780. 116th Cong., 2d sess. Introduced in House February 6, 2020. https://www.congress.gov/116/bills/hr5780/BILLS-116hr5780rfs.pdf.

U.S. Library of Congress. Congressional Research Service. *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, by Brian E. Humphreys. R45809. 2019.

U.S. Library of Congress. Congressional Research Service. *Somalia*, by Lauren Ploch Blanchard. IF10155. 2020.

U.S. President. Proclamation. "Enhancing Vetting Capabilities and Processes for Detecting Attempted Entry into the United States by Terrorists or Other Public-Safety Threats, Proclamation 9645 of September 24, 2017." *Federal Register* 82, no. 186 (September 27, 2017): 45161-45172. https://www.govinfo.gov/content/pkg/FR-2017-09-27/pdf/2017-20899.pdf.

U.S. Senate. *A Resolution Establishing the Select Committee on Cybersecurity*. S. Res. 23. 115th Cong., 1st sess. Introduced in Senate January 24, 2017. https://www.congress.gov/115/bills/sres23/BILLS-115sres23is.pdf.

U.S. Senate. Committee on Homeland Security and Governmental Affairs. *Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report: Permanent Subcommittee on Investigations*. 112th Cong., 1st sess., October 3, 2012. https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

U.S. Senate. Committee on Homeland Security and Governmental Affairs. *Focus on Fusion Centers: A Progress Report: Hearing before the Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness*. 110th Cong., 2d sess., April 17, 2008. S. Hrg. 110-694.

U.S. Senate. Committee on Homeland Security and Governmental Affairs. *Securing America's Future: The Cybersecurity Act of 2012: Testimony before the Committee on Homeland Security and Governmental Affairs*. 112th Cong., 2d sess., February 16, 2012.

U.S. Senate. *Cybersecurity Act of 2012*. S 2105. 112th Cong., 2d sess. Introduced in Senate February 14, 2012. https://www.congress.gov/112/bills/s2105/BILLS-112s2105pcs.pdf.

U.S. Senate. *Cybersecurity Act of 2012.* S 3414. 112th Cong., 2d sess. Introduced in Senate July 19, 2012. https://www.congress.gov/112/bills/s3414/BILLS-112s3414pcs.pdf.

U.S. Senate. *Cybersecurity Vulnerability Identification and Notification Act of 2019*. S 3045. 116th Cong., 1st sess. Introduced in Senate December 12, 2019. https://www.congress.gov/116/bills/s3045/BILLS-116s3045rs.pdf.

U.S. Senate. *Small Business Advanced Cybersecurity Enhancements Act of 2018*. S. 2735. 115th Cong., 2d Sess. Introduced in Senate April 24, 2018. https://www.congress.gov/115/bills/s2735/BILLS-115s2735is.pdf.

U.S. Special Operations Command. *The Grey Zone*. Tampa, FL: U.S. Special Operations Command, 2015. https://www.soc.mil/swcs/ProjectGray/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf.

Venhaus, John M. *Why Youth Join al-Qaeda*. Special Report 236. Washington, DC: United States Institute of Peace, 2010. https://www.usip.org/publications/2010/05/why-youth-join-al-qaeda.

Vidino, Lorenzo. *Countering Radicalization in America: Lessons from Europe.* Special Report 262. Washington, DC: United States Institute of Peace, 2010. https://www.usip.org/sites/default/files/resources/SR262%20-%20Countering_Radicalization_in_America.pdf.

Watkins, Michael D. "How to Think Strategically." *Harvard Business Review*, April 20, 2007. https://hbr.org/2016/12/4-ways-to-improve-your-strategic-thinking-skills.

White House. *Empowering Local Partners to Prevent Violent Extremism in the United States*. Washington, DC: White House, 2011. https://www.hsdl.org/?view&did=682863.

White House. *America First: A Budget Blueprint to Make America Great Again, Budget of the United States Government, Fiscal Year 2018*. Washington, DC: Office of Management and Budget, 2017. https://www.govinfo.gov/content/pkg/BUDGET-2018-BUD/pdf/BUDGET-2018-BUD.pdf.

White House. *Budget of the United States Government, Fiscal Year 2019*. Washington, DC: Office of Management and Budget, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf.

White House. *Budget of the United States Government, Fiscal Year 2020*. Washington, DC: White House, 2019. https://www.govinfo.gov/content/pkg/BUDGET-2020-BUD/pdf/BUDGET-2020-BUD.pdf.

White House. *Budget of the United States Government, Fiscal Year 2021*. Washington, DC: White House, 2020. https://www.whitehouse.gov/wp-content/uploads/2020/02/budgetfy21.pdf.

White House. *National Security Strategy*. Washington, DC: White House, 2010. http://nssarchive.us/national-security-strategy-2010/.

White House. *National Security Strategy*. Washington, DC: White House, 2015. http://nssarchive.us/national-security-strategy-2015/.

White House. *National Security Strategy*. Washington, DC: White House, 2017. http://nssarchive.us/national-security-strategy-2017/.

White House. *National Strategy for Counterterrorism*. Washington, DC: White House, 2011. https://www.hsdl.org/?view&did=487985.

White House. *National Strategy for Counterterrorism*. Washington, DC: White House, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.

White House. *National Strategy to Secure Cyberspace*. Washington, DC: White House, 2003. https://www.hsdl.org/?view&did=1040.

White House. *Report on the Legal and Policy Frameworks Guiding the United States' Use of Military Force and Related National Security Operations*. Washington, DC: White House, 2016. https://www.hsdl.org/?view&did=798033.

White House. *Strategic Implementation for Empowering Local Partners to Prevent Violent Extremism in the United States*. Washington, DC: White House, 2011. https://www.hsdl.org/?view&did=694059.

White House. *U.S. Strategy Toward Sub-Saharan Africa*. Washington, DC: White House, 2012. https://www.hsdl.org/?view&did=712667.

Wise, Rob. *Al Shabaab*. Washington, DC: Center for Strategic and International Studies, 2011. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/110715_Wise_AlShabaab_AQAM%20Futures%20Case%20Study_WEB.pdf.

Yihun, Belete Belachew. "Ethiopian Foreign Policy and the Ogaden War: The Shift From 'Containment' to 'Destabilization,' 1977-1991." *Journal of Eastern African Studies* 8, no. 4 (2014): 677-691. https://doi.org/10.1080/17531055.2014.947469.

Youngstown Sheet & Tube Co. v. Sawyer. 343 U.S. 579 (1952).

Zimmerman, Katherine, and Jacqulyn Meyer Kantack, Colin Lahiff and Jordan Indermuehle. *US Counterterrorism Objectives in Somalia: Is Mission Failure Likely?* Washington, DC: American Enterprise Institute, 2017. https://www.criticalthreats.org/wp-content/uploads/2017/03/US-Counterterrorism-Objectives-in-Somalia.pdf.

Vita

Nick Urbonowicz is a U.S. Army noncommissioned officer currently serving as a Congressional Defense Fellow in the U.S. Senate. He holds a bachelor's in American history from the State University of New York Empire State College and a master's in legislative affairs from George Washington University.